MTR110176

MITRE TECHNICAL REPORT

Threat Assessment & Remediation Analysis (TARA)

Methodology Description
Version 1.0

Sponsor: OSD (NII)
Dept. No.: G021
Contract No.: W15P7T-10-C-F600
Project No.: 031180SE-K1

Jackson Wynn
Joseph Whitmore
Geoff Upton
Lindsay Spriggs
Dan McKinnon
Richard McInnes
Richard Graubart
Lauren Clausen

Bedford, MA

October 2011

Report Documentation Page	*Form Approved OMB No. 0704-0188*

1. REPORT DATE **OCT 2011**	2. REPORT TYPE	3. DATES COVERED **00-00-2011 to 00-00-2011**

4. TITLE AND SUBTITLE **Threat Assessment & Remediation Analysis (TARA): Methodology Description Version 1.0**	5a. CONTRACT NUMBER 5b. GRANT NUMBER 5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER 5e. TASK NUMBER 5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **The MITRE Corp,7515 Colshire Dr,McLean,VA,22102**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR’S ACRONYM(S) 11. SPONSOR/MONITOR’S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

Mission Assurance Engineering (MAE) is the sub discipline of Enterprise Systems Engineering (ESE) intended to provide mission assurance against the advanced persistent threat (APT). The APT uses an evolving set of tactics, techniques, and procedures (TTPs) to establish and maintain a foothold in the enterprise’s information infrastructure, and to exploit that foothold to ex-filtrate large volumes of sensitive information, to corrupt mission-critical information, and/or to deny or degrade mission capabilities. This report describes the Threat Assessment & Remediation Analysis (TARA) methodology, which applies MAE to systems and acquisitions. TARA is a methodology to identify and assess cyber threats and select countermeasures effective at mitigating those threats. When applied in conjunction with a Crown Jewels Analysis (CJA) or other means for assessing mission impact, CJA and TARA together provide for the identification, assessment, and security enhancement of mission critical assets, which is the cornerstone of mission assurance.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**60**	

This page intentionally left blank.

Abstract

Mission Assurance Engineering (MAE) is the sub discipline of Enterprise Systems Engineering (ESE) intended to provide mission assurance against the advanced persistent threat (APT). The APT uses an evolving set of tactics, techniques, and procedures (TTPs) to establish and maintain a foothold in the enterprise's information infrastructure, and to exploit that foothold to ex-filtrate large volumes of sensitive information, to corrupt mission-critical information, and/or to deny or degrade mission capabilities. This report describes the Threat Assessment & Remediation Analysis (TARA) methodology, which applies MAE to systems and acquisitions. TARA is a methodology to identify and assess cyber threats and select countermeasures effective at mitigating those threats. When applied in conjunction with a Crown Jewels Analysis (CJA) or other means for assessing mission impact, CJA and TARA together provide for the identification, assessment, and security enhancement of mission critical assets, which is the cornerstone of mission assurance.

Executive Summary

The ESE Capstone Program fosters improved enterprise integration and interoperability across the DoD and IC enterprises by conducting systems engineering activities that complement and shape the existing FFRDC work program with sponsors from across the enterprises. The FY11 Mission Assurance Engineering (MAE) Capstone task develops a methodology called Cyber Risk Remediation Analysis (CRRA) for selecting countermeasures (CMs) effective at mitigating cyber threats attributable to the Advanced Persistent Threat (APT).

This report builds upon a FY10 ESE Capstone task that defined a methodology called Cyber Threat Susceptibility Analysis (CTSA) [1] to identify and rank a system's susceptibility to cyber attacks mounted by APT threat actors. The APT can be summarized as an adversary with the sophistication and resources to apply multiple attack vectors to achieve its objectives, which include establishment of footholds within a targeted information technology (IT) infrastructure.

The combined approach of CTSA followed by CRRA is referred to as Threat Assessment & Remediation Analysis (TARA), which is a system level engineering practice within the MITRE Mission Assurance Engineering (MAE) portfolio. The objective of MAE is to reduce risk to mission attributable to the APT. The objective of this paper is to define a rigorous and repeatable methodology for performing TARA assessments, and to describe the framework of tools, data, and workflows that collectively support this practice.

Table of Contents

List of Figures

This page intentionally left blank.

1 Introduction

This paper details a methodology resulting from a two (2) year ESE Capstone effort to develop an engineering methodology that promotes greater mission assurance within the system acquisition lifecycle.

1.1 Motivation

This research is motivated in part by a 2008 report by the Air Force Scientific Advisory Board (SAB) on "Defending and operating in a Contested Cyber Domain", which defines mission assurance (MA) as "*measures that are required to accomplish objectives of missions in the presence of information assurance compromises*." [2]

Mission assurance assumes that the adversary, herein referred to as the Advanced Persistent Threat (APT), has the motivation, skills, and resources necessary to breach/penetrate security perimeters and gain persistent access to cyber assets within an enterprise. NIST SP 800-39 defines the APT as "*an adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors (e.g., cyber, physical, and deception). These objectives typically include establishing and extending footholds within the information technology infrastructure of the targeted organizations for purposes of ex-filtrating information, undermining or impeding critical aspects of a mission, program, or organization; or positioning itself to carry out these objectives in the future. The advanced persistent threat: (i) pursues its objectives repeatedly over an extended period of time; (ii) adapts to defenders' efforts to resist it; and (iii) is determined to maintain the level of interaction needed to execute its objectives*." [3]

Mission assurance enables mission success in the presence of the APT by establishing a "fight through" capability through the use of resilience and maneuverability. Resilience refers to the ability to provide and maintain an acceptable level of service in the face of faults and challenges to normal operation. It has also been characterized as an emergent property that allows complex systems to absorb external stresses, to recognize, anticipate, and defend against evolving risks, or to adaptively respond to avoid potential losses. The SAB report defines maneuverability as the ability for cyber defense to adapt to threats as quickly as the type and nature of the threats themselves change, thereby making the outcome of each step taken by the attacker less certain and less predictable.

The SAB report asserts that information assurance activities within the system acquisition lifecycle are necessary but not sufficient to achieve mission assurance for a number of reasons. First, the traditional approach used within the acquisition lifecycle to characterize threats, i.e., via System Threat Assessment (STA) reporting, is not designed to capture constantly changing and evolving threats, such as cyber threats. Additionally, no security measure or control is foolproof against all threats, which means that the possibility of an Information Assurance (IA) compromise can be minimized but never eliminated entirely. One conclusion of the SAB report is that a fundamental change is needed in how cyber threats are managed within the context of the systems acquisition lifecycle. The methodology detailed in this paper, Threat Assessment & Remediation Analysis (TARA), is intended to help satisfy this need.

1.2 An Overview of TARA

Threat Assessment & Remediation Analysis (TARA) is an engineering methodology to identify, prioritize, and respond to cyber threats through the application of countermeasures that reduce

susceptibility to cyber attack. TARA is a system level engineering practice within the MITRE Mission Assurance Engineering (MAE) portfolio, which is described in Section 1.3.1 below.

Aspects of the TARA methodology are illustrated in the following diagram:

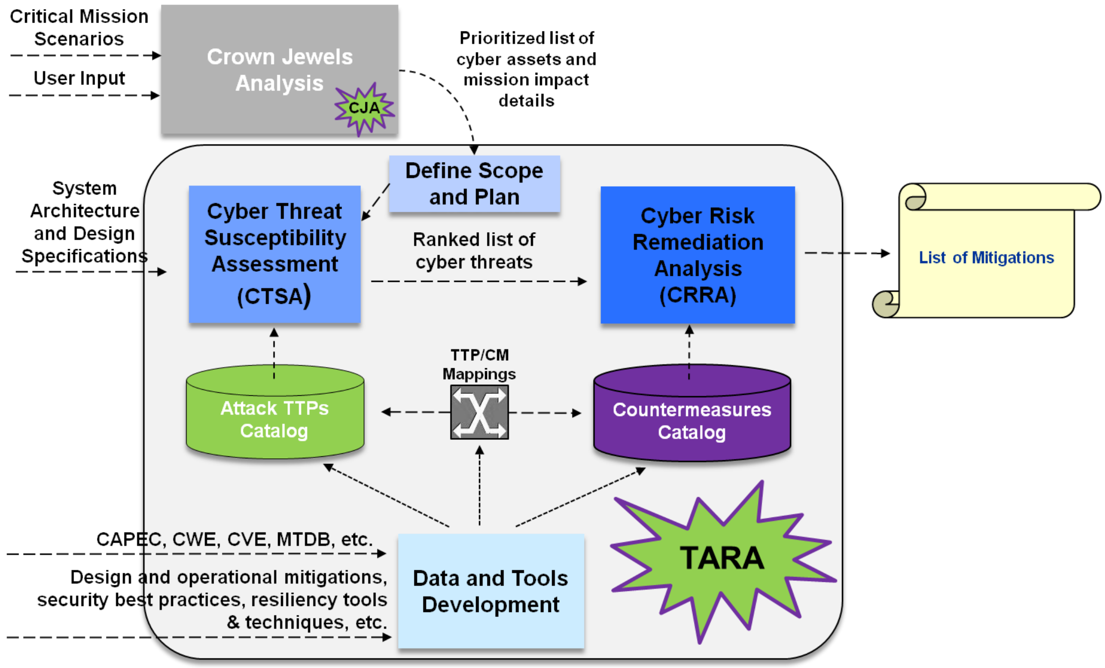

Figure 1 Threat Assessment & Remediation Analysis (TARA) Methodology

The TARA methodology includes three (3) activities: Cyber Threat Susceptibility Analysis (CTSA), Cyber Risk Remediation Analysis (CRRA), and Data and Tools development. These activities support three (3) workflows: TARA assessments, catalog development, and toolset development.

A TARA assessment is a sponsor-directed workflow to evaluate selected cyber assets using information about known adversarial Tactics, Techniques, and Procedures (TTPs) and Countermeasures (CMs) stored in catalogs.

Each TARA assessment involves a three (3) step process: establish assessment scope in terms of the cyber assets and range of TTPs to evaluate, apply CTSA to assess a cyber asset's susceptibility to attack over the range of TTPs, and conduct CRRA to determine the set of CMs that will effectively reduce or eliminate the cyber asset's susceptibility to attack. A TARA assessment delivers recommendations that help program managers make informed decisions on how to make systems more resilient and less vulnerable once deployed. Details about the TARA assessment approach are found in Section 2.1 of this document.

TARA assessments can be conducted independently or as follow-on to a Crown Jewels Analysis (CJA) [4] or similar mission impact assessment in which mission critical cyber assets are identified. A TARA assessment that evaluates mission critical cyber assets can provide mission assurance value early in the acquisition lifecycle.

Catalog and toolset development are workflows internal to the TARA methodology that ensure the currency of TTP and CM catalogs and their mappings, as well as the software tools that

support the application of the methodology. Details about these workflows are found in Sections 2.2 and 2.3 of this document.

Key features of the TARA methodology include:

- TARA assessments can be performed on deployed systems or on systems still in their acquisition lifecycle.
- Use of stored catalogs of TTPs and CMs promote consistency from one TARA assessment to the next
- TTP and CM catalog data is derived from open source and classified sources, and can be selectively partitioned/filtered based on the scope of the TARA assessment
- TARA is not a one-size-fits-all approach; the level of rigor applied in assessments can be adjusted up or down as necessary
- The TARA toolset provides default scoring tools to quantitatively assess TTP risk and CM cost effectiveness. These tools can be tailored or omitted entirely based on the assessment scope and/or the needs of the program.

The last two points above support the objective that TARA provides a flexible assessment approach. The complete assessment methodology may be too heavy-weight to be practical for some programs. Functional subsets of the methodology, referred to as TARA-lite approaches, are discussed in Section 4.

1.3 Related Work

1.3.1 The Mission Assurance Engineering (MAE) Portfolio

The MAE portfolio is comprised of an ever-evolving collection of Enterprise Systems Engineering (ESE) practices that combine practical experience, information sharing, research, and experimentation to help sponsors better address the APT.

1.3.1.1 Cyber-Aware Enterprise Transformation Strategies

This group of practices, which includes Cyber Prep [5], establishes a framework and methodology for grounding an organization’s cyber security investment strategy in an understanding of, and an organizational stance toward, the APT.

1.3.1.2 Cyber Resiliency Engineering

Cyber resiliency engineering applies resilience strategies and techniques to the processes, personnel, and individual systems that support mission capabilities. These strategies and techniques, collectively referred to as Resilient Architecture for Mission Assurance and Business Objectives (RAMBO) [6], are developed under auspices of the Center for Resiliency Experimentation, which is funded through the MITRE Innovation Program.

1.3.1.3 System/Acquisition Mission Assurance Engineering (SAMAE)

SAMAE applies knowledge of the APT to the system acquisition process, focusing on the System Development Lifecycle (SDLC). TARA and CJA both fall within the SAMAE focus area.

1.3.1.4 Information Systems Security Engineering (ISSE)

ISSE focuses on achieving the security objectives of confidentiality, integrity, availability, and accountability in the context of a broad range of threats that include, but are not focused on, the APT.

1.3.2 TARA-like Methodologies in Industry

Methodologies to assess cyber risk and evaluate mitigations similar to TARA have been developed in industry and academia. A partial list of these methodologies includes the following. Detailed comparisons of these methodologies with TARA are provided in Section 4.6.

1.3.2.1 Mission Oriented Risk and Design Analysis (MORDA)

MORDA [7] is a mission-oriented risk assessment methodology developed for NSA for use during the system development lifecycle. Analysis of the MORDA approach is detailed in Section 4.6.1.

1.3.2.2 Decision Analysis to Counter Cyber Attacks (DACCA)

DACCA [8] was a FY09-FY10 MITRE MOIE to develop a decision analysis process and model to aid in the selection of mitigations for cyber attacks. Analysis of the DACCA approach is detailed in Section 4.6.2.

1.3.2.3 Common Vulnerability Scoring System (CVSS)

CVSS [9] provides a quantitative model that can be used to score/assess the risk associated with reported vulnerabilities. The CVSS model is detailed in Section 4.6.3.

1.3.2.4 Microsoft Threat Modeling

Microsoft [10, 11] developed a threat modeling methodology to systematically identify and rate cyber threats during the system development lifecycle. The Microsoft approach is discussed in Section 4.6.4.

1.4 Outline of this Paper

This rest of this paper is organized as follows. Section 2 details the TARA methodology, including TARA assessment, catalog, and toolset development workflows. Section 3 provides a worked example of a TARA assessment performed on selected COTS cyber assets using a limited set of twenty five (25) TTPs and associated countermeasures. Section 4 discusses aspects of the TARA methodology, including TARA-lite approaches and TARA-like approaches found in industry. Common definitions and additional details on the catalog schema and TARA toolset are provided as Appendices.

2 Threat Assessment & Remediation Analysis (TARA)

This section details the TARA methodology, the TTP and CM catalogs, and the software tools that are used to develop and utilize catalog data.

2.1 Assessment Methodology

TARA assessments are conducted on selected cyber assets. A cyber asset is defined as any IT asset used to store, transport, and/or process information within an enterprise, including servers, clients systems, network appliances, etc.

The objectives of a TARA assessment are:

- To identify and prioritize high-risk adversarial Tactics, Techniques, and Procedures (TTPs) that a cyber asset may be susceptible to,
- To identify and prioritize countermeasures (CMs) effective against those TTPs, and
- To recommend CMs that can reduce the susceptibility of a cyber asset to attack.

Each TARA assessment is comprised of two analysis steps:

- Cyber Threat Susceptibility Assessment (CTSA)
- Cyber Risk Remediation Analysis (CRRA)

The CTSA step identifies and evaluates the susceptibility of a cyber asset to attack relative to a set of TTPs, while the CRRA step identifies a set of countermeasures that reduce the susceptibility or lessen the effects of a cyber attack.

The deliverable of a TARA assessment is a set of recommended steps to reduce or minimize susceptibility of a cyber asset to attack. One goal for these recommendations is to establish traceability of a CM to the TTP that it mitigates, and to the cyber asset and the mission capability (or capabilities) made more resilient through application of the CM. This traceability allows program managers to make informed choices when selecting which CMs to implement in a given program.

2.1.1 Cyber Threat Susceptibility Assessment (CTSA)

CTSA quantitatively assesses a system's inability to resist cyber attack over a range of adversary Tactics, Techniques, and Procedures (TTPs) and produces a Threat Matrix, which provides a ranked list of TTPs that each cyber asset is susceptible to. This matrix is used in Cyber Risk Remediation Analysis (CRRA), discussed in the next subsection, to select the range of TTPs to mitigate.

CTSA consists of the following steps:

1. Establish assessment scope
2. Identify candidate TTP
3. Eliminate implausible TTPs
4. Apply scoring model
5. Construct the threat matrix

2.1.1.1 Establish Assessment Scope

The first step in CTSA is to establish the scope of the evaluation, which can be characterized in terms of:

- The set of system assets being evaluated
- The range of attack TTPs being considered
- The types of adversaries

When CTSA is conducted as follow-on to a Crown Jewels Analysis (CJA), the set of system assets within the scope of the assessment may include all identified crown jewel cyber assets, i.e., cyber assets whose compromise would seriously impair mission capability or readiness. If the CTSA is being conducted independently or in the absence of the CJA, the list of cyber assets may be arbitrary or may include a presumptive list of crown jewel cyber assets.

The range of TTPs considered in CTSA may include but is not limited to cyber, electronic warfare (EW), and supply chain. A cyber attack is an attack via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information. Electronic warfare refers to military action involving the use of electromagnetic and directed energy weapons to control the electromagnetic spectrum or to deny its use by the enemy. Supply chain attacks allow the adversary to utilize implants or other vulnerabilities inserted into hardware or software prior to installation in order to exfiltrate data, or disrupt information technology hardware, software, operating systems, peripherals (information technology products) or services at any point during the life cycle.

Types of adversaries considered in CTSA may include external adversaries, insiders, and trusted insiders. The distinction among these relates to the adversary's proximity to the targeted system. A security perimeter separates an external adversary from an internal adversary, i.e., an insider. This perimeter can take the form of a firewall, a DMZ, a locked door, and so on. Once the security perimeter is breached, however, the external adversary has gained insider access. Similarly, an insider is distinguished from a trusted insider by the level of access granted, i.e., a trusted insider may have physical or administrative access that an unprivileged user does not. Enforcement of least privilege separates insiders from trusted insiders, who may have opportunities to apply a wider range of attack TTPs than insiders or external adversaries. The scope of a CTSA assessment may include or exclude TTPs attributable to each type of adversary.

2.1.1.2 Identify Candidate TTP

Once the scope of CTSA is established, the next step is to evaluate the cyber asset's architecture, technology, and security capabilities against TTPs in the MAE Catalog. Unclassified sources of adversary TTPs in the catalog include MITRE-hosted resources such as Common Attack Pattern Enumeration and Classification (CAPEC), Common Weakness Enumeration (CWE), and Common Vulnerability Enumeration (CVE) [12, 13, and 14]. CAPEC is a compilation of attack patterns derived from specific real-world incidents. In this context, the terms "adversarial TTP" and "attack pattern" are considered synonymous. CWE is a catalog of software weaknesses and defects that adversarial TTPs may exploit. CVE catalogs vulnerabilities found in COTS hardware and software products. The list of candidate TTPs developed in a TARA assessment may include TTPs derived from these sources.

2.1.1.3 Eliminate Implausible TTPs

This initial set of candidate TTPs undergoes a narrowing process to eliminate TTPs considered implausible. Several factors can make a TTP an implausible method of cyber attack. Many TTPs have prerequisites or conditions that must hold true in order for that TTP to be effective. A prerequisite for a SQL injection attack, for example, is that the system must include a SQL

database. Use of weak passwords is one condition that must hold true in order for an adversary to successfully conduct brute force password attacks. Many candidate attack TTPs may be eliminated because of missing prerequisites.

It is also possible to eliminate candidate attack TTPs by making assumptions about the system's security posture. For example, DoD systems undergo the DIACAP Certification and Accreditation (C&A) process [15] to verify that all required security controls are implemented. One set of security controls requires that the system's configuration be hardened using DISA-published Security Technical Implementation Guides (STIGs) [16]. Certain attack TTPs may not be plausible for systems that have been hardened in accordance with these STIGs.

2.1.1.4 Apply Scoring Model

Candidate TTPs that cannot be eliminated are ranked using a scoring model. The TTP scoring model assesses the risk associated with each TTP relative to other plausible TTPs considered in the assessment. This ranking helps set priorities on where to apply security measures to reduce the system's susceptibility to cyber attack. A default TTP scoring spreadsheet is illustrated in Figure 2 below.

Factor Range	1	2	3	4	5
Proximity: What proximity would an adversary need in order to apply this TTP?	no physical or network access required	protocol access through DMZ and firewall	user account to target system (no admin access)	admin access to target system	physical access to target system
Locality: How localized are the effects posed by this TTP?	isolated to single unit	single unit and supporting network	external networks potentially impacted	all units in theater or region	all units globally and associated infrastructure
Recovery Time: How long would it take to recover from this TTP once the attack was detected?	< 10 hours	20 hours	30 hours	40 hours	> 50 hours
Restoration Costs: What is the estimated cost to restore or replace affected cyber asset?	< $10K	$25K	$50K	$75K	> $100K
Impact: How serious an impact is loss of data confidentiality resulting from successful application of this TTP?	no impact from TTP	minimal impact	limited impact requiring some remediation	remediation activities detailed in COOP	COOP remediation activites routinely exercised
Impact: How serious an impact is loss of data integrity resulting from successful application of this TTP?	no impact from TTP	minimal impact	limited impact requiring some remediation	remediation activities detailed in COOP	COOP remediation activites routinely exercised
Impact: How serious an impact is loss of system availability resulting from successful application of this TTP?	no impact from TTP	minimal impact	limited impact requiring some remediation	remediation activities detailed in COOP	COOP remediation activites routinely exercised
Prior Use: Is there evidence of this TTP in the MITRE Threat DB?	no evidence of TTP use in MTDB	evidence of TTP use possible	confirmed evidence of TTP use in MTDB	frequent use of TTP reported in MTDB	widespread use of TTP reported in MTDB
Required Skills: What level of skill or specific knowledge is required by the adversary to apply this TTP?	no specific skills required	generic technical skills	some knowledge of targeted system	detail knowledge of targeted system	knowledge of both mission and targeted system
Required Resources: Would resources be required or consumed in order to apply this TTP?	no resources required	minimal resources required	some resources required	significant resources required	resources required and consumed
Stealth: How detectable is this TTP when it is applied?	not detectable	detection possible with specialized monitoring	detection likely with specialized monitoring	detection likely with routine monitoring	TTP obvious without monitoring
Attribution: Would residual evidence left behind by this TTP lead to attribution?	no residual evidence	some residual evidence, attribution unlikely	attribution possible from characteristics of the TTP	same or similar TTPs previously attributed	signature attack TTP used by adversary

Figure 2 Default TTP Risk Scoring Spreadsheet

This spreadsheet assesses TTP risk based on a range of criteria that include impact, restoration costs, down time, level of sophistication, likelihood for attribution, and so on. This list of criteria has evolved over time. Organizations may, and are encouraged to, tailor the scoring model to reflect their needs. But whatever scoring model is employed must be used consistently. Use of the same scoring model provides a common basis for comparing and ranking TTPs based on relative risk. TTP risk scores derived using different scoring models are not comparable.

In the default scoring model, a uniform range of values [1...5] is assigned to each criteria. For criteria such as impact, a higher value results in a higher TTP risk score. These contributing factors appear in blue in the scoring model spreadsheet. For criteria such as level of

sophistication, a higher value results in a lower TTP risk score. These mitigating factors appear in red in the scoring model spreadsheet. Implicit in this scoring model is an adversary threat model that assumes a high degree of sophistication reduces the likelihood of occurrence, leading to a lower overall risk score. Tailoring the scoring model may be necessary to reflect a particular adversary threat model.

The default scoring model supports different criteria having different weightings. Some criteria may be more significant to the overall risk score than others. For a system that processes classified data, for example, a higher weighting is assigned to loss of confidentiality than for a system that processes unclassified data. TTP risk scores are calculated based on the criteria value assignments and associated criteria weightings. This calculation yields a TTP risk score in the range [1...5], with the value five (5) signifying a TTP that poses the greatest risk.

It should be noted that assessor biases will affect the TTP scoring no matter which scoring model is used. Scoring model weightings and values are assigned by an assessor based on his/her background and experience; no two assessors will arrive at the same risk score for a given TTP. To address this issue, multiple assessors may be needed to help normalize these biases.

2.1.1.5 Construct a Threat Matrix

CTSA produces a Threat Matrix, which lists plausible attack TTPs ranked by decreasing risk score and their mapping to cyber assets as a function of adversary type. The Threat Matrix may also be used to tabulate an aggregate susceptibility to cyber attack for each cyber asset considered in the assessment. This matrix is used in the follow-on Cyber Risk Remediation Analysis (CRRA) to identify potential mitigation strategies to address TTP susceptibilities. An example Threat Matrix is illustrated in Figure 3.

TTP ID	Risk Score	Cyber Asset #1			Cyber Asset #2		
		External	Insider	Trusted Insider	External	Insider	Trusted Insider
T000017	4.4		4.4	4.4		4.3	4.3
T000030	4.2		4.1	4.1		4.1	4.1
T000039	3.6	3.6	3.6			3.6	
T000041	3.2	3.2	3.2		3.2	3.2	
T000053	3.0						3.0
T000064	2.9				2.9		
T000086	2.6				2.6	2.6	2.6
T000127	2.6				2.6		
T000018	2.3					2.3	2.3
T000022	2.3	2.3	2.3	2.3	2.3	2.3	2.3
T000023	2.3	2.3	2.3		2.3	2.3	
T000029	2.2	2.2	2.2		2.2	2.2	
T000048	2.0			2.0			
T000054	1.9				1.9	1.9	
T000063	1.6				1.6	1.6	
T000065	1.3	1.3					
Aggregate Susceptibility		14.9	22.1	12.8	21.6	30.4	18.6
		49.8			70.6		

Figure 3 TARA Threat Matrix

The example Threat Matrix above evaluates two (2) cyber assets over a range of sixteen (16) attack TTPs, which are scored using the default TTP scoring model from Figure 2. If a cyber asset is susceptible to a TTP, its risk score is transferred to that cyber asset. Aggregate susceptibility is then tabulated for each cyber asset and adversary type. In this example, Cyber Asset #2 is more susceptible than Cyber Asset #1, particularly to external cyber threats. For presentation purposes, colors are used to bin TTPs into severity categories based on risk score, as follows:

- TTPs with a risk score in the range [4.0…5.0] pose serious risk and appear in red,
- TTPs with a risk score in the range [2.5…3.9] pose moderate risk and appear in yellow, and
- TTPs with a risk score in the range [1.0…2.4] pose minimal risk and appear in blue.

2.1.2 Cyber Risk Remediation Analysis (CRRA)

Cyber Risk Remediation Analysis (CRRA) is an approach for selecting countermeasures (CMs) to reduce a cyber asset's susceptibility to attack over a range of Tactics, Techniques, and Procedures (TTPs) associated with the APT.

The term countermeasure (CM) is defined in CNSS 4009 [17] as *an action, device, procedure or technique that opposes or counters a threat, a vulnerability, or an attack by eliminating or preventing it, by minimizing the harm it can cause, or by detecting and reporting it so that corrective action can be taken. The selection of CMs is governed by the system lifecycle of the cyber asset being evaluated. Recommended CMs are those judged to be effective at mitigating TTPs that a cyber asset may be susceptible to, and may include changes to requirements, system design, testing, deployment configuration, and/or operating procedures*.

CRRA is performed separately for each cyber asset and consists of the following steps:

1. Select which TTPs to mitigate
2. Identify plausible countermeasures
3. Assess countermeasure merit
4. Identify an optimal CM solution
5. Prepare recommendations

2.1.2.1 Select which TTPs to Mitigate

The first step is to select a list of TTPs to mitigate. There are several strategies to perform this selection. One strategy is to focus only on the highest scoring TTPs in the Threat Matrix for each cyber asset. Another strategy is to focus on the cyber asset(s) that have the highest aggregate susceptibility. A third strategy is to focus exclusively on crown jewel cyber assets. A hybrid strategy might select high scoring TTPs for the crown jewel cyber assets with the highest aggregate susceptibility. Whatever strategy is used, the result will be a list of TTPs for each cyber asset being assessed.

Applying this strategy to the Threat Matrix in Figure 3, a list of TTPs that pose the greatest cyber risk to Cyber Asset #2 might be: T000017, T000030, T000039, T000041, T000053, T000064, T000086, and T000127. This list includes TTPs for both external and internal (insider) threat actors that pose high to moderate risk to that cyber asset. Applying this same selection strategy to Cyber Asset #1 yields a different set of TTPs, however, which is why CRRA is performed for each cyber asset.

2.1.2.2 Identify Plausible Countermeasures

CRRA employs a mapping table to represent the many-to-many mapping between TTPs and countermeasures (CMs). This mapping is used to identify candidate CMs for a given set of TTPs. The TTP/CM mapping table for the above list of high risk TTPs for Cyber Asset #2 is illustrated in Figure 4.

In a TTP/CM mapping table, each row corresponds to a countermeasure and each column corresponds to a TTP. Each mapping of CM to TTP is characterized by the mitigation effectiveness of the CM over a range of criteria: detect, neutralize, limit, and recover. Detect CMs serve to identify or uncover the action or presence of a TTP. Neutralize CMs stop or prevent execution of a TTP. Limit CMs serve to reduce or constrain the risk associated with a TTP, either by lessening the severity or likelihood. Recovery CMs facilitate recovery from attack. A given CM may be highly effective at detecting a certain TTP, moderately effective at neutralizing or limiting its impact, but provide no mitigation value in recovering from its effects.

CM ID	Mitigation Effectiveness (by TTP ID)							
	T000017	T000030	T000039	T000041	T000053	T000064	T000086	T000127
C000039						NM		
C000045		NH	NH					
C000047			NH					
C000058			NH					
C000067	DL,NM							
C000073				LM				
C000083	LH,NH							
C000086				LM				
C000096				NM				
C000097				DM,NM				
C000110				LM,NL				
C000113				NM				
C000121							DM,NM	
C000122				NM				
C000124			LM					
C000126					LM			
C000129							NM	
C000133						NM		
C000144			NH					
C000145	NH		NH					
C000147		NM						
C000159						NM		
C000164		NM						
C000165				LH				
C000173		NM						
C000187								LM
C000188		NM						

Figure 4 TTP/CM Mapping Table

A 2-character notation denotes mitigation effectiveness in the TTP/CM mapping table, where the first character signifies the type of mitigation from the list: (N)eutralize, (D)etect, (L)imit and (R)ecover. The second character represents the degree of effectiveness from the list: (L)ow, (M)edium, (H)igh, and (V)ery high. For example, NH is the 2-character notation to represent Neutralize-High mitigation effectiveness. Figure 5 below enumerates the entire notation.

Effectiveness	Mitigation Category			
	Detect	Neutralize	Limit	Recover
Very High	DV	NV	LV	RV
High	DH	NH	LH	RH
Medium	DM	NM	LM	RM
Low	DL	NL	LL	RL

Figure 5 Mitigation Effectiveness Notations

Not all CMs in the TTP/CM mapping table for a given set of TTPs may be a plausible mitigation for the system or program being assessed. A given CM may be disqualified for a variety of reasons. Some CMs in the MAE Catalog are specific to a particular technology or architecture not being utilized in the system. Other CMs in the MAE Catalog are specific to a particular phase of the system engineering life cycle, which may have already occurred. A CM that calls for design verification activities, for example, would not be plausible for a system that is already operational. Conversely, a TARA assessment may identify CMs that are already implemented or applied as security measures in the system being assessed. In this case, the CM should be "carried on the books" through the analysis to verify whether it provides sufficient mitigation value over the range of TTPs being assessed.

2.1.2.3 Assess Countermeasure Merit

The objective of CRRA is to identify an optimal list of CMs for a specified range of TTPs. To identify an optimal list of CMs, it is first necessary to assess the relative merit of each CM. The approach detailed in this report calculates a utility/cost (U/C) ratio for each CM, based on information in the MAE Catalog, and uses these U/C ratios to rank CMs based on their relative merit.

A utility/cost (U/C) ratio is a “bang-for-buck” valuation of a CM derived from its estimated utility and cost. To assess the utility of each CM, a score is assigned to each mitigation effectiveness notation, as illustrated in Figure 6. The utility of each CM can now be calculated by summing the scores over the range of TTPs mitigated. For example, the utility score for a CM that the TTP/CM mapping table identifies as NH for 2 TTPs and LM for 1 TTP would be 2*9 + 5 = 23, based on the scores assigned in Figure 6. It should be noted that the scoring used in this example imposes a bias that assigns greater mitigation value to Neutralize and Limit CMs than to Detect and Recover CMs. This scoring may be tailored to suit the needs of an assessment.

Ordinal Value	Mitigation Effectiveness Scoring			
	Detect	Neutralize	Limit	Recover
Very High	DV=7	NV=11	LV=9	RV=7
High	DH=5	NH=9	LH=7	RH=5
Medium	DM=3	NM=7	LM=5	RM=3
Low	DL=1	NL=5	LL=3	RL=1

Figure 6 Mitigation Effectiveness Scoring

The second factor in calculating the U/C ratio is CM cost. The cost of a CM should consider the cost to develop, integrate, and maintain the CM over the operational life of the system. Whatever model is used to assess cost, its valuation should map to a linear scale of [1...5] in order to be used to calculate U/C ratios. Default cost values are assigned to CMs in the MAE Catalog, which may need to be adjusted to reflect realistic costs for the program or system being assessed.

A CM Ranking Table can facilitate the calculation of U/C ratios over the range CMs identified in a TTP/CM mapping table. The CM Ranking Table example in Figure 7 below corresponds to the TTP/CM mapping table in Figure 4. The table is constructed by inverting the contents of the TTP/CM mapping table and adding some columns to tabulate the CM merit scoring. U/C ratios are calculated for each CM once utility and cost values have been assigned. The last step to construct this table is to order the rows by decreasing U/C ratio.

CM ID	Neutralize			Limit		Detect		CM Merit Scoring		
	NH=9	NM=7	NL=5	LH=7	LM=5	DM=3	DL=1	Utility	Cost	U/C Ratio
C000159		T000064						7	1	7.0
C000164		T000030						7	1	7.0
C000165				T000041				7	1	7.0
C000173		T000030						7	1	7.0
C000188		T000030						7	1	7.0
C000045	T000030, T000039							18	3	6.0
C000145	T000039, T000017							18	3	6.0
C000083	T000017			T000017				16	3	5.3
C000073					T000041			5	1	5.0
C000067		T000017					T000017	8	2	4.0
C000096		T000041						7	2	3.5
C000113		T000041						7	2	3.5
C000133		T000064						7	2	3.5
C000097		T000041				T000041		10	3	3.3
C000110			T000041		T000041			10	3	3.3
C000047	T000039							9	3	3.0
C000058	T000039							9	3	3.0
C000144	T000039							9	3	3.0
C000086					T000041			5	2	2.5
C000121		T000086				T000086		10	4	2.5
C000124					T000039			5	2	2.5
C000126					T000053			5	2	2.5
C000187					T000127			5	2	2.5
C000039		T000064						7	3	2.3
C000122		T000041						7	3	2.3
C000129		T000086						7	3	2.3
C000147		T000030						7	3	2.3

Figure 7 CM Ranking Table

A more sophisticated approach to assess CM merit might use a scoring model similar to the TTP scoring model, detailed in the previous section, to numerically assess CM merit based on a variety of weighted criteria. The U/C ratio is a simplified version of this approach, which calculates a ratio of one contributing factor (utility) to one mitigating factor (cost). CRRA does not mandate use of either U/C ratios or a CM scoring model; any approach for estimating CM merit may be used provided it is used to uniformly assess all CMs.

2.1.2.4 Identify an Optimal CM Solution

An optimal CM solution is the set of CMs that provides effective mitigation over a specified range of TTPs at the lowest cost. What constitutes "effective mitigation" is determined by a CM selection strategy. A CM selection strategy establishes a basis for filtering the range of potential solutions, i.e., the solution space, which can grow exponentially with the number of CMs. For example, a CM selection strategy could require that the following conditions hold in order to qualify as a viable solution:

1. At least one highly effective CM must be selected for each TTP
2. Less effective CMs may be combined to satisfy #1.
3. A Detect CM is required for TTPs that have no Neutralize CMs

The CM selection strategy reduces the range of viable CM solutions to a manageable number. More restrictive selection strategies may be employed to further constrain the solution space for a given assessment. For example, a more restrictive selection strategy might require two highly effective CMs for each TTP or require that a Detect CM is mandatory for each TTP, even for TTPs that have Neutralize CMs. A CM selection strategy can be so restrictive that no viable CM solutions exist given the TTPs, CMs, and mapping data contained in the catalog. A viable solution does not exist for TTPs T000053 or T000127 using the CM selection strategy listed above applied to the TTP/CM mapping table in Figure 4, for example.

Identification of an optimal CM solution can be performed manually by walking the CM Ranking table. Combinations of CMs that satisfy the CM selection strategy are recorded in a CM solutions list, as illustrated in Figure 8.

Solution	Countermeasures (CMs)										Cost
1	C000045	C000083	C000121	C000126	C000129	C000165	C000187				18
2	C000113	C000121	C000122	C000126	C000129	C000144	C000164	C000173	C000187		21
3	C000058	C000096	C000113	C000121	C000126	C000129	C000147	C000173	C000187		22
4	C000047	C000096	C000097	C000121	C000126	C000129	C000145	C000147	C000164	C000187	26

Figure 8 CM Solutions List

The last step is to tabulate the total cost of each solution by summing the costs of its constituent CMs. The lowest cost solution will be optimal over the range of solutions identified. Manual analysis is not a viable approach for large solution spaces. However a near-optimal solution can still be identified with some work. One heuristic to facilitate early identification of a [near] optimal solution is to start from the top of the CM ranking table once CMs are sorted by decreasing U/C ratios, with the premise that optimal CM solutions contain proportionally more CMs with high U/C ratios.

2.1.2.5 Prepare Recommendations

The final CRRA step is to translate the CM solution list into well-formed recommendations. A well-formed recommendation includes three (3) pieces of information:

1. The action, device, procedure or technique recommended, i.e., which CM to be applied
2. The reason why the CM is required, i.e., the TTPs that it mitigates
3. The implication or effect if the CM is not applied, i.e., the potential impact to mission capability resulting from compromise of the cyber asset

The selected CMs together with the TTP/CM Mapping table address the first two items above. In order to address all three elements, however, a crown jewel analysis or similar mission impact assessment may be needed in order to ascertain the potential mission impact that may result from compromise of the cyber asset.

2.2 The MAE Catalog

The MAE Catalog stores adversarial Tactics, Techniques, and Procedures (TTPs) and the Countermeasures (CMs) that mitigate them. The MAE data model represents and defines the catalog's internal representation. In the TARA assessment workflow, catalog data is filtered and searched based on properties defined in the data model, using search tools provided by the MAE toolset. In the catalog development workflow, catalog data on TTP and CMs is collected from a variety unclassified and classified sources and loaded into the catalog, using tools provided by the MAE toolset.

2.2.1 The MAE Data Model

The MAE Catalog implements the data model illustrated in Figure 9. Entities in the MAE data model include TTPs, CMs, Asset Classes (ACs), and the many-to-many mappings that interconnect these entities. These entities are described below, with additional details and attribute descriptions provided in Appendix C.

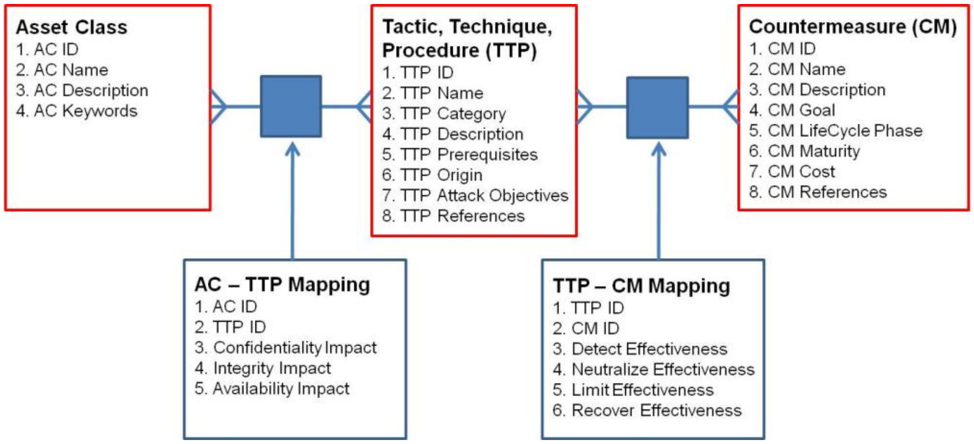

Figure 9 MAE Data Model

2.2.1.1 Tactics, Techniques, and Procedure (TTP)

A TTP is defined as a sequence of steps performed by a cyber threat actor to conduct a cyber attack. Categories of TTP include cyber, Electronic Warfare (EW), supply chain, which target technologies, and social engineering, which targets system users and operators.

TTPs are often characterized by the level of sophistication and resources required to be applied. While TTPs that require APT-level sophistication and resources are a focus for the catalog, TARA can be used to assess susceptibility to TTPs regardless of the level of sophistication they require.

2.2.1.2 Countermeasure (CM)

A countermeasure (CM) is defined as actions, devices, procedures, or techniques that meet or oppose (i.e., counters) a threat, a vulnerability, or an attack by eliminating or preventing it, by minimizing the harm it can cause, or by discovering and reporting it so that corrective action can be taken.

Some CMs may be specific to the lifecycle phase of the cyber asset, e.g., methodology, development practices, system requirements, architecture, design, testing, training, lifecycle support, etc. The lifecycle phase of the cyber asset will often determine the range of CM that provide "actionable" recommendations, i.e., recommendations that can be applied in the timeframe of the assessment.

Other factors for excluding (or including) CMs are technical maturity or cost. High technical maturity may be a key consideration when selecting CMs for systems that are operationally deployed. However CMs derived from present-day research may be very appropriate for acquisition programs where Initial Operational Capability (IOC) is 3-4 years away.

2.2.1.3 Asset Class (AC)

An Asset Class (AC) establishes a basis for grouping related TTPs. The MAE Catalog includes asset classes to represent architectural elements and types of technology. TTPs mapped to these asset classes correspond to associated attack vectors. Examples of technology asset classes include database, web server, software, network protocol, etc. TTPs associated with the database asset class, for example, include SQL injection, blind SQL injection, etc., as these are customary attack vectors of database technology. There is presently no hierarchical nesting or ontology imposed on asset classes in the MAE catalog. Also, a TTP may be mapped to any number of asset classes.

A variation on the asset class concept is the shopping cart, which is an asset class created to represent a cyber asset being evaluated in a TARA assessment. TTPs associated with a shopping cart are those considered plausible attack vectors for the cyber asset.

Keywords may be associated with an asset class. Searches for these keywords in system documentation establish linkage between the cyber asset being evaluated, an asset class, and the TTPs that a given technology may be susceptible to.

2.2.1.4 TTP/CM Mapping

The TTP/CM mapping represents the many-to-many relationship between TTPs and CMs within the MAE Catalog. This many-to-many relationship recognizes that a given TTP may be mitigated by numerous CMs, and that a given CM may mitigate numerous TTPs.

Different CMs have different mitigation objectives, which include neutralizing the TTP, limiting its impact, detecting when the TTP can or is occurring, and/or facilitating system recovery after the cyber attack has occurred.

The effectiveness with which a CM achieves these mitigation objectives varies from one TTP to the next. In the data model mitigation effectiveness is represented as a property of the TTP/CM mapping and used as the basis for estimating the utility of a CM.

2.2.2 Sources of Catalog Data

The MAE catalog includes TTP data from a variety of open source and classified sources, including Common Attack Pattern Enumeration and Classification (CAPEC), Common Weakness Enumeration (CWE), Common Vulnerabilities and Exposures (CVE), Cyber Prep, and classified security incident reporting. Other sources of TTP data include BlackHat [18] and SchmooCon [19] presentations.

Classified TTP and CM data is stored in a collateral SECRET instance of the MAE Catalog. Both the unclassified and classified instances of the MAE catalog conform to the MAE data model and schema detailed in this paper.

CM data is derived from a variety of unclassified sources and imported into the MAE catalog. These sources include CAPEC, CWE, industry practices, Resilient Architecture for Mission Assurance and Business Objectives (RAMBO) prototype initiatives, etc.

2.2.3 MAE Catalog Development

The cyber threat landscape is constantly changing as APTs develop new TTPs to exploit system weaknesses, and as new CMs are developed to mitigate them. MAE catalog development is an ongoing necessity to ensure that TARA assessments have available the latest information on TTPs and CMs.

2.2.3.1 Developing Catalog TTPs, CMs, and TTP/CM Mappings

TTP and CM data stored in the MAE catalog is updated when TTPs or CMs are created or deleted, and as details change. TTP/CM mappings are created when new uses for existing CMs are identified, or to revise mitigation effectiveness data.

2.2.3.2 Developing Asset Classes and AC/TTP Mappings

Asset Class data stored in the MAE catalog is updated to as new Asset Classes are identified, as associated keyword lists are maintained, and as new AC/TTP mappings are identified. Catalog development also includes creation of shopping carts and the mappings of a shopping cart to TTPs deemed plausible in a TARA assessment.

2.3 MAE Toolset

The MAE toolset provides a range of capabilities that support TARA assessments and the development of MAE catalog data. Catalog development and search, report generation, and scoring tools are all supported. Appendix D includes screen shots for some of the tools detailed in this section.

The toolset integrates Apache Solr [20] to provide text search of catalog data, a MySQL database to support report generation, and the Windows IIS web server and .NET framework to provide Web-based catalog data management and report generation. The toolset also integrates Microsoft Excel spreadsheet templates.

2.3.1 Catalog Development Tools

Catalog development tools include web forms used to create, modify, delete, and search catalog data, and automated support for importing TTP and CM data stored in spreadsheets and XML files and exporting catalog data as XML files.

2.3.1.1 Data Entry Web Forms

Web forms are used to manually enter and edit catalog data for TTPs, CMs, and ACs. These forms provide fields to enter text data, and checkboxes and drop down lists for fields that contain fixed enumerations. Each TTP, CM, and AC is assigned a unique ID. These IDs are automatically generated by the web form when new catalog entries are created, and used to retrieve entries already stored in the catalog.

TTP/CM and/or AC/TTP mapping data may be manually entered using one of these manual data entry forms, or using the TTP-CM mapping tool. Existing mappings may be modified and deleted using the same interface. Appendix D includes screen shots of these web forms.

2.3.1.2 Catalog Data Import Tools

The toolset supports capabilities to import catalog data from external sources that include Microsoft Excel spreadsheets and XML data files. An Excel spreadsheet template can be used to collect TTP, CM, and TTP/CM mapping data when manual data entry is not possible. The toolset menu includes a data import tool, which is used to import data from the Excel spreadsheet template. This tool functions by converting the Excel spreadsheet contents to an intermediate XML format that can be imported. Additional XSLT filters can be crafted to convert XML data in other formats to the intermediate XML format used by the MAE toolset.

2.3.1.3 Catalog Data Export Tools

The toolset maintains a collection of XML files, each representing a TTP, CM, AC, or mapping that is created in the catalog. These XML files conform to the MAE catalog XML schema outlined in Appendix C. The XML data export capability is used to transfer catalog data from one MAE catalog to another.

2.3.2 Catalog Search Tools

Catalog search tools are provided to support TARA assessment activities. These tools are used to search for specific TTPs, CMs, and mapped associations of TTPs and CMs over a range of search criteria. Capabilities are also provided to save, store, and reuse catalog searches.

2.3.2.1 TTP Search Web Form

The toolset provides a web form that is used to search TTP data in the catalog. This TTP search tool operates in two (2) search modes: Asset Class search and manual search. In Asset Class search mode, TTP entries associated with a specified set of Asset Classes are returned. In manual search mode, TTP entries that match specified catalog properties are returned. In both modes the list of TTP fields returned can be specified. Query results can be copied and pasted into Microsoft office products, e.g., spreadsheets, word documents, power point presentations, etc.

2.3.2.2 CM Search Web Form

The toolset provides a web form that is used to search CM data in the catalog. This CM search tool also operates in two (2) search modes: TTP collection search and manual search. TTP collection search accepts a list of TTPsas input and produces a list of CMs that are mapped to the specified TTPs. Manual CM search returns CM catalog entries that match specified catalog properties. In both modes the list of CM fields returned can be specified. Query results can be copied and pasted into Microsoft office products.

2.3.3 Report Generation

The TARA methodology makes use of a variety of data formats, tables, and matrices. The report generation capability provides automation to assist in the creation of intermediate formats used to construct final reports and artifacts.

The sensitivity of certain TARA artifacts may require that they be produced manually on a classified system in their final form. With DoD systems, for example, a table that associates TTPs with a system that is deployed is typically handled as classified data. Report generation capabilities within the toolset are constrained to ensure that classified data cannot be automatically generated. Less sensitive, intermediate formats may be constructed from catalog data through automated report generation, however, without compromising the security of deployed systems.

2.3.4 Scoring Tools

The MAE toolset includes an Excel spreadsheet that implements a default scoring model used to assess TTP risk. This spreadsheet is illustrated in Figure 2.

3 Worked Example

This section demonstrates application of the TARA assessment methodology.

3.1 Assessment Scope

Sections 2.1.1.1 and 2.1.1.2 define the scope of CTSA in terms of the cyber assets evaluated against a specified range of TTPs. This worked example evaluates two (2) Commercial, Off-the-Shelf (COTS) products against twenty-five (25) TTPs selected from the open source CAPEC catalog. Specific details about the products considered in this example are omitted from the discussion.

3.1.1 Cyber Assets

3.1.1.1 LAN Switch

The LAN Switch provides wire-rate, 10 gigabit connectivity and full IPv4 and IPv6 support with unicast and multicast switching and routing, including native support of OSPF, IGMPv3, and PIM protocols, and advanced quality of service (QoS) prioritization. This device supports both Web-based and agent-based (SNMP) network management capabilities and can operate over extreme range of environmental conditions.

3.1.1.2 VOIP Gateway

The VOIP Gateway is a fully-integrated multi-service voice switch that supports any-to-any gateway functionality to provide enterprise VoIP capabilities. Product features include simplified operation and reduced set up time to facilitate deployment to end users. It can support secure, encrypted voice and data via LAN, cellular or satellite uplinks, and includes bandwidth optimization features that help minimize transmissions overhead over remote or satellite connections.

3.1.2 Range of TTPs

Figure 10 lists the twenty five (25) CAPEC attack patterns used in this worked example.

ID	TTP Name	Source Reference
1	Subverting Environment Variable Values	CAPEC-13
2	Target Programs with Elevated Privileges	CAPEC-69
3	Cryptanalysis	CAPEC-97
4	XQuery Injection	CAPEC-84
5	SQL Injection through SOAP Parameter Tampering	CAPEC-110
6	Using Escaped Slashes in Alternate Encoding	CAPEC-78
7	Subvert Code-signing Facilities	CAPEC-68
8	Cross Site Tracing	CAPEC-107
9	HTTP Request Smuggling	CAPEC-33
10	HTTP Request Splitting	CAPEC-105
11	Brute Force	CAPEC-112
12	Manipulating Writeable Configuration Files	CAPEC-75
13	Overflow Buffers	CAPEC-100

14	Forced Integer Overflow	CAPEC-92
15	Filter Failure through Buffer Overflow	CAPEC-24
16	Exploiting Trust in Client (aka Make the Client Invisible)	CAPEC-22
17	Accessing/Intercepting/Modifying HTTP Cookies	CAPEC-31
18	Session Credential Falsification through Prediction	CAPEC-59
19	Postfix, Null Terminate, and Backslash	CAPEC-53
20	Lifting Data Embedded in Client Distributions	CAPEC-37
21	Using Unicode Encoding to Bypass Validation Logic	CAPEC-71
22	Simple Script Injection	CAPEC-63
23	Cross Site Request Forgery (aka Session Riding)	CAPEC-62
24	Man in the Middle Attack	CAPEC-94
25	Malicious Software Download	CAPEC-185

Figure 10 Worked Example TTPs

3.2 Cyber Threat Susceptibility Assessment (CTSA)

3.2.1 TTP Plausibility

Section 2.1.1.3 details the approach used to evaluate the plausibility of candidate TTPs. The table in Figure 11 assesses the plausibility of each of TTPs listed above as attack vectors for the LAN Switch and VOIP Gateway, based on a review of available product documentation.

ID	TTP Name	Source Reference	LAN Switch		VOIP Gateway	
			Plausible?	Rationale	Plausible?	Rationale
1	Subverting Environment Variable Values	CAPEC-13	yes	The device runs a variant of Unix as its embedded OS and supports a variety of interactive shells including SSH. It is common for user interactive shells to support environment variables.	yes	Adminstrative tools used to manage device are installed and run on Windows platforms, and may utilize environment variables within the Windows operating environment.
2	Target Programs with Elevated Privileges	CAPEC-69	yes	It is common for Unix-based systems to support OS-defined execution permissions and OS utility programs that operate with elevated execution privileges.	yes	The CLI supports privilege levels 0 - 15. CLI commands can be invoked during a CLI session to change the user's current privilege level. It may be possible to initiate a privilege escalation through an undocumented backdoor or exploitation of CLI commands
3	Cryptanalysis	CAPEC-97	yes	A variety of router protocols supported in this device make use of encryption as a basis for authenticating other devices. Encryption also used to protect passwords and shared secrets.	yes	The system can be configured with one or more media crypto class objects used to provide secure voice capabilities for audio streams that transit the device. It may also be possible to conduct traffic analysis using call logging data stored on the device.
8	Cross Site Tracing	CAPEC-107	yes	There is no indication from the available documentation that web server refuses HTTP TRACE requests. Browser clients support session cookies and use of javascript.	no	There is no indication in the documentation that the device or its administrative applications support or utilize http-based protocols or web server technology.
9	HTTP Request Smuggling/Splitting	CAPEC-33/105	yes	If an ACL policy is defined to filter HTTP protocol requests from specified subnets or MAC addresses, it may be possible for a "chunked" HTTP request containing HTTP requests from multiple endpoints to transit the filter without being detected.	no	There is no indication in the documentation that the device or its administrative applications support or utilize http-based protocols or web server technology.
11	Brute Force	CAPEC-112	yes	Success depends on the length of shared secrets and/or passwords that the device is configured with. For peer authentication in supported router protocols, an 8 character ascii password may be set. The default value is NULL.	yes	Device is configured to use RADIUS shared secrets. Passwords associated with user accounts may or may not have strength/complexity restrictions, depending on deployment. Success of brute force guessing subject to enforcement of these restrictions.
12	Manipulating Writeable Configuration Files	CAPEC-75	yes	The switch's configuration file can be modified externally and loaded into the switch through its automatic download capability.	yes	Configuration files can be modified in and downloaded into remote devices. These files store configuraiton data as ascii text.
13	Overflow Buffers	CAPEC-100	yes	CVE catalog lists 6 buffer overflow vulnerabilities relating to this product, resulting in denial of service, privilege escalation, and arbitary code execution.	yes	There are no documented CVEs associated with this device or its software. It is still plausible however that buffer overflow defects exist as 0-day exploits.
15	Filter Failure through Buffer Overflow	CAPEC-24	yes	Some of the CVE listed buffer overflows above are attributed to long requests, session cookies, and/or credential strings.	yes	There are no documented CVEs associated with this device or its software. It is still plausible however that buffer overflow defects exist as 0-day exploits.
16	Exploiting Trust in Client (aka Make the Client Invisible)	CAPEC-22	yes	The origin of remote user connections is not validated by the device following authentication.	yes	All VX device management conducted remotely using either telnet to access the CLI or adminstrative tools, e.g, vxbuilder, vxwatch, etc. Telnet sessions are not protected from eavesdropping and may be subject to replay or spoofing. Vxapplications likely use an proprietary API to abstract the communications protocols, which may also be susceptible to

17	Accessing/Intercepting/ Modifying HTTP Cookies	CAPEC-31	yes	Remote WebView sessions utilize cookies to store and exchange user credentials. No assumptions can be made regarding the client browser's storage of cookies or the ability to intercept and/or modify cookie data exchanged between the browser client and WebView.	no	There is no indication in the VX documentation that the device or its administrative applications support or utilize http-based protocols or web server technology.
23	Cross Site Request Forgery (aka Session Riding)	CAPEC-62	yes	A browser client could connect to an external website that downloads malicious browser code that takes control of the session to exfiltrate or corrupt device configuration settings.	no	There is no documented thin-client or browser-based interface to this device.
24	Man in the Middle Attack	CAPEC-94	yes	Strong mutual authentication is not performed between a client browser and the device when establishing a session. Use of SSL to encrypt session traffic is a configuration option that is not enabled by default.	yes	Certificate-based, strong mutual authentication using TLS is supported. However use of self-signed client certificates can be enabled. Using self-signed certificates allows a user to use the TLS transport encryption, but bypass authentication.
25	Malicious Software Download	CAPEC-185	yes	TFTP and SFTP can be used to download an image file from a local or remote host filesystem location to the flash directory.	yes	Adminsrative privilege is needed in order to FTP a new software image (.tbz format) to the device and to telnet to the device to run the install command through the CLI.
4	XQuery Injection	CAPEC-84	no	No indication that the devices supports or utilizes XML data formats.	no	No indication that the devices supports or utilizes XML data formats.
5	SQL Injection through SOAP Parameter Tampering	CAPEC-110	no	No indication that the device supports SOAP-based web services.	no	No indication that the device supports SOAP-based web services.
6	Using Escaped Slashes in Alternate Encoding	CAPEC-78	no	Slash and backshash characters used as field/parameter delimiters for selected CLI commands. They do not used to select an alternative encoding.	yes	Router table input rules support use of backslash as an escape character.
7	Subvert Code-signing Facilities	CAPEC-68	no	The device supports in-service software upgrades (ISSUs) of OS image files that are not validated using MD5 checksums.	no	Code signing and/or image file validation usng MD5 checksums is not supported.
14	Forced Integer Overflow	CAPEC-92	no	Documentation describes CLI command line validation that includes error messaging for out of bounds numeric input parameters	no	Documentation specifies value ranges for many integer parameters. It is reasonable to assumed that the CLI and/or admin tools validate input against these ranges.
18	Session Credential Falsification through Prediction	CAPEC-59	no	There is no indication that session cookies are generated deterministically and/or can be known in advance.	no	There is no indication that the device utilizes session cookies.
19	Postfix, Null Terminate, and Backslash	CAPEC-53	no	There is no indication that the device supports alternative representations for NULL. Command line delimiters supported by the CLI include |, \, /, -, _, and space.	no	There is no indication that the device supports alternative representations for NULL.
20	Lifting Data Embedded in Client Distributions	CAPEC-37	no	This TTP targets client systems.	yes	Admin tools installed on a remote Windows host may retain user account info that can be lifted from the client.
21	Using Unicode Encoding to Bypass Validation Logic	CAPEC-71	no	There is no indication that the device accepts or rejects input in unicode format. Input data detailed in documentation is identified to be in ascii format.	no	There is no indication that the device supports data in unicode format.
22	Simple Script Injection	CAPEC-63	no	This TTP targets client systems. The device could be a source for script injection attacks that target client browsers with malicious javascript incorporated into WebView web pages.	yes	An unauthorized script could be associated with a trunk group and invoked when an inbound call is received to place a call to a compromised remote location

Figure 11 TTP Plausibility

3.2.2 TTP Risk Scoring

Section 2.1.1.4 discusses the default scoring model used in CTSA. For the worked example, the default TTP scoring model was tailored to eliminate several factors in the scoring calculation by assigned them zero weighting. These eliminated factors include adversary skills and resources, TTP detection, and potential attribution. The resulting scoring model spreadsheet appears in Figure 12 below.

Factors for assessing TTP Risk						Factor Value [1…5]	Factor Weight
Factor Range	1	2	3	4	5		
How localized are the effects posed by this TTP?	no noticeable effects	effects limited to targeted asset	targeted asset and supporting network	noticable effects to external enclave/domain	effects experienced globally	1	0.2
How long would it take to recover from this TTP once the attack was detected?	no recovery needed	< 1 hour	< 24 hours	< 72 hours	> 72 hours	1	0.1
What is the estimated cost to restore or replace affected cyber asset?	no restoration required	< $10K	< $20K	< $50K	> $50K	1	0.1
How serious an impact is loss of data confidentiality resulting from successful application of this TTP?	no adverse effects	limited adverse effects	serious adverse effects	severe adverse impact	catastrophic impact	1	0.2
How serious an impact is loss of data integrity resulting from successful application of this TTP?	no adverse effetcs	limited adverse effects	serious adverse effects	severe adverse impact	catastrophic impact	1	0.2
How serious an impact is loss of system availability resulting from successful application of this TTP?	no adverse effects	limited adverse effects	serious adverse effects	severe adverse impact	catastrophic impact	1	0.2
Is there evidence of this TTP's use in a security incident database?	Incident database not consulted	evidence of TTP use possible	confirmed evidence of TTP use in database	frequent use of TTP reported	widespread use of TTP reported	0	0
What level of skill or specific knowledge is required by the adversary to apply this TTP?	no specific skills required	generic technical skills	some knowledge of targeted system	detail knowledge of targeted system	knowledge of both mission and targeted system	0	0
Would resources be required or consumed in order to apply this TTP?	no resources required	minimal resources required	some resources required	significant resources required	resources required and consumed	0	0
How detectable is this TTP when it is applied?	not detectable	detection possible with specialized monitoring	detection likely with specialized monitoring	detection likely with routine monitoring	TTP obvious without monitoring	0	0
Would residual evidence left behind by this TTP lead to attribution?	no residual evidence	some residual evidence, attribution unlikely	attribution possible from characteristics of the TTP	same or similar TTPs previously attributed	signature attack TTP used by adversary	0	0

Figure 12 Tailored TTP Scoring Model

3.2.3 Threat Matrix

Section 2.1.1.5 details the final step of CTSA to create a Threat Matrix. The Threat Matrix prepared for the worked example is illustrated in Figure 13 below. It was generated by applying the TTP scoring model from Figure 13 to the list of plausible TTPs in section 3.2.2. In the Threat Matrix below, high-risk TTPs serious risks appear in red and moderate risk TTPs appear in yellow. The mapping of TTPs to threat actors, e.g., external, insider, and/or trusted insider, estimates the proximity of the adversary to the cyber asset that is minimally needed to conduct the TTP.

TTP ID	TTP Name	Source Reference	Risk Score	LAN Switch			VOIP Gateway		
				External	Insider	Trusted Insider	External	Insider	Trusted Insider
25	Malicious Software Download	CAPEC-185	4.3			4.3			4.3
22	Simple Script Injection	CAPEC-63	4.2	4.2	4.2	4.2		4.2	4.2
12	Manipulating Writeable Configuration Files	CAPEC-75	4.1			4.1			4.1
24	Man in the Middle Attack	CAPEC-94	3.8		3.8	3.8		3.8	3.8
15	Filter Failure through Buffer Overflow	CAPEC-24	3.6	3.6	3.6	3.6	3.6	3.6	3.6
13	Overflow Buffers	CAPEC-100	3.6	3.6	3.6	3.6	3.6	3.6	3.6
2	Target Programs with Elevated Privileges	CAPEC-69	3.5	3.5	3.5		3.5	3.5	
1	Subverting Environment Variable Values	CAPEC-13	3.5		3.5	3.5		3.5	3.5
11	Brute Force	CAPEC-112	3.3	3.3	3.3		3.3	3.3	
23	Cross Site Request Forgery (aka Session Riding)	CAPEC-62	3.3		3.3	3.3			
3	Cryptanalysis	CAPEC-97	3.2	3.2			3.2	3.2	3.2
6	Using Escaped Slashes in Alternate Encoding	CAPEC-78	3.2					3.2	3.2
20	Lifting Data Embedded in Client Distributions	CAPEC-37	3.0				3.0	3.0	
9	HTTP Request Smuggling/Splitting	CAPEC-33/105	2.8	2.8	2.8				
17	Accessing/Intercepting/Modifying HTTP Cookies	CAPEC-31	2.8	2.8	2.8				
16	Exploiting Trust in Client (aka Make the Client Invisible)	CAPEC-22	2.7	2.7	2.7		2.7	2.7	
8	Cross Site Tracing	CAPEC-107	2.5	2.5	2.5	2.5			
			Aggregate Scores	32	40	33	23	38	34
				105			94		

Figure 13 Threat Matrix

3.3 Cyber Risk Remediation Analysis (CRRA)

3.3.1 TTPs to Mitigate

Section 2.1.2.1 outlines different strategies for selecting TTPs to evaluate in CRRA. These strategies all make use of the ranked list of TTP in the Threat Matrix from the previous section. This worked example focuses on the top ranked TTPs in the Threat Matrix for the LAN Switch. Figure 14 lists the TTPs from the Threat Matrix.

LAN Switch	TTP Description
CAPEC-185	Malicious Software Download
CAPEC-63	Simple Script Injection
CAPEC-75	Manipulating Writeable Configuration Files
CAPEC-94	Man in the middle
CAPEC-24	Filter Failure through Buffer Overflow
CAPEC-100	Buffer Overflow

Figure 14 Threat Matrix

3.3.2 Candidate Countermeasures (CMs)

As discussed in 2.1.2.2, a TTP/CM mapping table identifies candidate countermeasures (CMs) for a specified list of TTPs. Each CM to TTP mapping is characterized by the mitigation value the CM provides over a range of criteria including detect, neutralize, limit, and recover. A 2-character notation is used to represent mitigation effectiveness within the mapping table, where the first character signifies the type of mitigation from the list: (N)eutralize, (D)etect, (L)imit and (R)ecover. The second character represents the degree of effectiveness from the list: (L)ow, (M)edium, (H)igh, and (V)ery high. Figure 15 depicts the TTP/CM mapping table for the TTPs listed above.

Countermeasure (CM)			Mitigation Effectiveness (by CAPEC ID)					
ID	Name	Cost	100	75	24	185	94	63
C001	Use ASLR	Low	NM					
C002	Programming language selection	Medium	NH					
C003	Use vetted APIs	Medium	NM					NM
C004	Run software with least privilege	Low	RM			NM,RM		
C005	Run software in a sandbox	Low	RM		NM	NM,RM		
C006	Perform input validation	Low	NM		NH,RH			NM
C007	Use cryptographic checksums	Medium		DH		DH	DH,NH	
C008	Apply parser-based validation	Low		DL				
C009	Perform white list / black list validation	Low		LM				DM
C010	Restrict access to source repository and image file	Low		NM				
C011	Automated logging of configuration changes	Low		DL				
C012	Perform bounds check	Low			NH,RH			
C015	Monitor application logs	Low			DH			
C016	Use encryption	Medium				NH		
C017	Perform reverse DNS lookups	Low				NM		
C021	Enforce mutual authentication	Medium					NH	
C022	Add message timestamps	Medium					DM,NM	
C024	Use trusted intermediaries / proxies	Medium					NL,LM	
C025	Incorporate challenge/response protocols	High					DH,NH,RM	
C026	Disable script execution in browser	Low						NM
C027	Apply character encoding rules	Medium						NL
C029	Cononicalize input	Low						NL
C032	Perform validation on clients and servers	Low						NM

Figure 15 TTP/CM Mapping Table

3.3.3 CM Scoring

Section 2.1.2.3 details an approach to assess the merit of CMs in order to identify an optimal solution that satisfies a particular CM selection strategy. This approach calculates a Utility / Cost (U/C) ratio for each CM based on mitigation effectiveness and cost data stored in the MAE catalog. A CM Ranking Table for the worked example based on the TTP/CM mapping above is depicted in Figure 16 below.

CM ID	Neutralize			Detect			Limit	Recover		CM Merit Scoring		
	NH=9	NM=7	NL=5	DH=5	DM=3	DL=1	LM=5	RH=5	RM=3	Utility	Cost	U/C Ratio
C006	24	100,63						24		28	2	14.0
C005		24,185							100,185	23	2	11.5
C007	94			75,185,94						24	3	8.0
C012	24							24		14	2	7.0
C004		185							100,185	13	2	6.5
C003		100,63								14	3	4.7
C025	94			94					94	17	4	4.3
C009					63		75			8	2	4.0
C001		100								7	2	3.5
C010		75								7	2	3.5
C017		185								7	2	3.5
C026		63								7	2	3.5
C032		63								7	2	3.5
C022		94			94					10	3	3.3
C024			94				94			10	3	3.3
C002	100									9	3	3.0
C016	185									9	3	3.0
C021	94									9	3	3.0
C015				24						5	2	2.5
C029			63							5	2	2.5
C027			63							5	3	1.7
C008						75				1	2	0.5
C011						75				1	2	0.5

Figure 16 CM Ranking Table

3.3.4 [Near] Optimal Solution Set

Section 2.1.2.4 outlines an approach to manually walk the CM Ranking table to identify CM solution sets that satisfy a CM selection strategy. For the working example, the CM selection strategy assumes that no CM is completely effective and that two or more CMs are required for each TTP. This CM selection strategy is consistent with a defense-in-depth approach to security. Manual analysis of the CM Ranking Table above resulted in the five (5) CM solutions listed in Figure 17 below.

Solution	List of Countermeasures									Cost
1	C004	C006	C005	C007	C009	C021				14
2	C006	C005	C007	C009	C021					13
3	C005	C012	C007	C009	C001	C026	C021			14
4	C012	C007	C009	C001	C017	C026	C003	C021	C015	17
5	C007	C009	C001	C017	C026	C003	C021	C006	C012	18

Figure 17 Solutions List

Solution 2 identifies a list of CMs that mitigate the list of TTPs with the lowest overall cost over the range of solutions evaluated. The worked example does not evaluate all possible solutions, however, so this solution is optimal only for the solutions visited.

3.3.5 TARA Recommendations

Section 2.1.2.5 discusses what constitutes a well-formed recommendation in terms of the information it contains. The worked example identifies five (5) recommendations, one for each CM listed in Solution 2 above:

1. Perform input validation. This countermeasure (C006) is highly effective at neutralizing buffer overflow attacks, e.g., CAPEC-100, CAPEC-24, etc. and script injection attacks, e.g., CAPEC-63, etc.
2. Run software in isolation. This countermeasure (C005) is moderately effective at both neutralizing and recovering from buffer overflow attacks, e.g., CAPEC-100, CAPEC-24, etc., and malicious software download attacks, e.g., CAPEC-128, etc.
3. Utilize cryptographic checksums. This countermeasure (C007) is highly effective at detecting a wide range of TTP, including malicious software download attacks (CAPEC-185), man-in-the-middle attacks (CAPEC-94), and attacks that exploit writeable configuration files, e.g., CAPEC-75.
4. Implement white list and black list validation checks in combination. This countermeasure (C009) is moderately effective at detecting script injection attacks, e.g., CAPEC-63.
5. Enforce mutual authentication. This countermeasure (C021) is highly effective at neutralizing Man-in-the-Middle attacks, e.g., CAPEC-94, etc.

The third element of a well formed recommendation details the impact or effect that results if the recommendations above are not heeded. While a TARA assessment can outline the impact of a successful cyber attack relative to the cyber asset, e.g., loss of use, loss of control, etc., a Crown Jewels Analysis (CJA) or similar mission impact assessment technique is often necessary in order to ascertain the potential impact to the range of missions that device supports.

4 Discussion

4.1 Genesis of the TARA Methodology

The TARA approach continues to evolve and mature in response to lessons learned from its application to DoD systems and acquisition programs. TARA extends the CTSA methodology developed in FY10 under ESE Capstone funding to include CRRA, in addition to catalog and toolset development support. An important lesson learned from prior application of CTSA alone is the need for follow-on mitigation engineering analysis, which is the objective of CRRA.

Catalog and toolset development workflows are incorporated into TARA in recognition of the importance that catalog data plays in providing high quality recommendations that provide value to the sponsor. A TARA assessment based on stale catalog data could potentially do more harm than good by making recommendations that do not consider the latest high risk TTPs and/or most effective CMs.

A second lesson learned from previous assessments is that existing open source catalogs of attack patterns, TTPs, weaknesses, vulnerabilities, etc., are not well suited for use with CTSA. These datasets are intended to support a variety of uses and contain a wealth of detail, much of which has limited value in a TARA assessment. The catalog utilized for TARA assessments includes summary extracts of relevant attack patterns and reported vulnerabilities, organized to eliminate redundancy, to promote consistency, and to support evaluation of TTP and CM catalog data in a way that scales well for TARA assessments.

Another lesson learned is that there is no generally accepted approach to rank TTPs or CMs. Several methodologies surveyed in this paper each define their own evaluation criteria for assessing TTPs. The TARA methodology provides default scoring models to assess TTP risk and CM merit, but does not require their use. The FY11 MAE Capstone task provides scoring

spreadsheets based on this default scoring model. Each program is free to tailor the default scoring models and tools supplied, or to define their own.

4.2 Assessment Tailoring

TARA provides a methodology framework that can be adapted as needed to suit a sponsor's program. Variations of the standard methodology, described previously, that provide less rigor and/or greater focus on specific TTPs may have special uses.

One variation is to focus the TARA assessment on a limited subset of TTPs and CMs from the catalog. For example, the TARA methodology could be adapted for use in Electronic Warfare (EW) analysis by limiting the scope of the assessment to EW-related TTPs, e.g., jamming, spoofing, direction finding, etc., and CMs designed to mitigate those threats, e.g., antennae design, Frequency Hopping Spread Spectrum (FHSS), Direct Sequence Spread Spectrum (DSSS), etc.

The level of rigor and comprehensiveness of a full TARA assessment may not be warranted for all systems and/or programs. A focused assessment that considers only a handful of TTPs might dispense with the TTP risk scoring step to further reduce the assessment level of effort. An assessment whose objective is to enumerate a full list of potential CMs might similarly dispense with CM merit scoring. A TARA-lite assessment refers to a short duration activity to evaluate a system against a small, pre-selected set of TTPs. The need for scoring in a TARA-lite assessment is determined in the context of defining the assessment scope.

4.3 Support to Acquisition Programs

The TARA methodology is intended to support mission assurance in acquisition programs. In all cases, this methodology makes use of technical details about a system in order to identify the range of TTPs that an APT may plausibly use to conduct a cyber attack, and the range of CMs that provide mitigation. Design specifications are an excellent source for these technical details; however such documents may not be available in the timeframe that the TARA assessment is performed.

In the absence of [or in addition to] system documentation, a dialog may be established between the TARA assessment team and system designers to obtain pertinent system details. This requires management's willingness to commit contractor resources to support the assessment. A TARA assessment cannot provide a quality result in the absence of system documentation, management support, and contractor cooperation.

4.3.1 Pre-PDR Support

A standard TARA assessment produces a Threat Matrix that maps TTPs to the cyber assets that are susceptible to them. This matrix cannot be constructed without knowledge of the cyber assets comprising the system. The cyber assets of a system are derived from its allocated baseline, which may not exist prior to the acquisition program's technical milestone such as Preliminary Design Review (PDR).

A variation of the TARA assessment approach may be performed in conjunction with program protection planning prior to PDR however. This form of TARA assessment evaluates the susceptibility of a program's Critical Program Information (CPI) and/or Critical Technologies (CTs) to a limited range of adversary TTPs, focusing on ex-filtration of critical system design information, reverse engineering of critical technologies, and/or implantation of malicious hardware/software through COTS supply chains. A TARA assessment conducted in conjunction

with program protection planning will consider a range of programmatic countermeasures to mitigate these TTPs.

4.3.2 PDR-to-CDR Support

A TARA assessment may be initiated at PDR time based on the system's preliminary architecture, as detailed in system level architectural and subsystem design specifications. These specifications are typically delivered by the vendor as preliminary drafts immediately prior to PDR. The objective of a TARA assessment conducted in this timeframe would be to evaluate the system architecture, identify design changes to neutralize or limit the impact of high risk TTP, and submit recommendations prior to CDR in order to influence the system's design.

4.3.3 Post-CDR Support

A TARA assessment can also be initiated later in the system development lifecycle, once a system's design has stabilized, using information provided in architectural, design, and detailed design specifications. The objective of a TARA assessment conducted in this timeframe would be to identify and recommend system installation and configuration changes, changes to operational processes and procedures, or possibly design changes to be rolled into future revisions of the system.

Another variation of the TARA approach is as precursor to a vulnerability assessment. In this context, CTSA identifies attack vectors based on review of system documentation, while CRRA identifies testing and verification techniques to apply during vulnerability testing to assess these attack vectors. Risk scoring may be used to rank TTPs, depending on the number of TTPs considered. Merit scoring of countermeasures would provide little value as countermeasures would correspond to the verification testing techniques to be applied.

4.3.4 Engineering Trade-off Studies

The TARA methodology provides a systematic approach for conducting engineering trade off studies and/or AoA analysis, which can provide value throughout the acquisition lifecycle whenever susceptibility to the APT is a serious concern. Examples of AoA deliverables might provide a comparison of the APT susceptibility of COTS products, similar to the worked example above, or provide a comparative "before and after" susceptibility assessment of a system to which CMs have been applied.

4.4 Support for Operational Cyber Defense

Support to cyber operations requires capabilities for real-time cyber threat detection, assessment, and mitigation in a production environment based on deployed sensors that provide situational awareness of active TTPs. The TARA methodology does not support a real time threat assessment and response capability. As a methodology framework, however, TARA could be adapted to include a specialized TTP catalog, sensors, scoring model, and additional tools to automate countermeasure selection.

4.5 Towards an Adversary Model

Unlike some of the other methodologies surveyed in this paper, TARA does not develop a formal adversary model for the APT. It does however make assumptions about what an APT may know about a targeted system and/or what an APT may do in order to collect that data.

One assumption is that the APT has the means to collect detailed technical knowledge of the target network architecture and deployed systems to devise novel attack TTPs, and has personnel dedicated to collecting this technical knowledge through a variety of sources including open source data, ex-filtration of data from contactor, DoD and/or Government networks, cyber reconnaissance activities, and possibly insider access.

An APT may attempt to penetrate a network through multiple entry points and may successfully gain access through exposed systems that are most susceptible. It is assumed that the APT would attempt to establish a permanent or durable means of access once it had gained initial access. It is also assumed that the APT would conduct post-entry reconnaissance to identify additional targets and/or extend its reach into internal network domains. These assumptions provide impetus for conducting TARA assessment on the most susceptible systems, rather than systems deemed crown jewel cyber assets, and place a premium on countermeasures implemented internally that are effective at detecting TTPs.

Consistent with the goal of "thinking like the attacker", the CTSA approach may parallel the approach that a would-be APT might perform, particularly in its evaluation of open source details about the target system. CTSA develops a profile of the target system initially through review of open source, public information about the system. This can be effective when evaluating COTS products whose vendors make product technical documentation freely available.

4.6 Comparison of TARA to other Methodologies

4.6.1 Mission Oriented Risk and Design Analysis (MORDA)

MORDA is a mission-oriented risk assessment methodology developed for NSA for use during the system development lifecycle. MORDA is based on Multiple Objective Decision Analysis (MODA) [21], which is a commonly used approach for performing analytic decision analysis. MODA supports decision makers who need to consider multiple, potentially conflicting inputs. As applied to risk assessment, this approach is used to qualitatively assess the benefits of applying a countermeasure to improve security, relative to the negative effect(s) to the user associated with that countermeasure.

The MORDA methodology makes use of three (3) models: an Adversary model, a User Value model, and a Service Provider model. In the adversary model, MORDA evaluates the adversary's attack preferences, and assumes the adversary will attempt to maximize attack impact while minimizing cost. The range of adversary types considered by MORDA include foreign intelligence services, information warriors, cyber terrorists/activists, hackers/crackers/script kiddies, malicious insiders, the press, organized crime/lone criminals, law enforcement, and industrial competitors. For each, attack trees are developed to assess mission impact resulting from a system compromise.

Other models are used to represent the User and Server Provider, where the objective is to maximize value to the User, i.e., meet user's performance objectives without being unduly hindered by countermeasures, whether or not the system is under cyber attack. MORDA defined methods used to assess CM value include aggregated value, optimization, and cost-benefit analysis. The goal is to find the best balance between positive and negative effects of mitigations.

These models make use of information on adversaries, attack patterns and characteristics, as well as countermeasure design options and characteristics. Development of these models requires the

participation of a variety of SMEs, including threat analysts, security analysts, and system and development engineers. This need for SMEs to develop these models makes MORDA a resource-intensive methodology, which limits its use to critical systems.

TARA is similar to MORDA in its application of a MODA-based analytic approach to scoring/assessing TTPs and CMs. In TARA, a system is evaluated using TTP and CM data stored in the MAE catalog, which is intended to be reused across TARA assessments. With MORDA, attack trees are developed to assess potential impact. It is not known whether attack trees can be reused across MORDA assessments.

Additionally, MORDA applies an adversary model that distinguishes nine (9) types of adversaries, including both APT and non-APT actors. TARA assessments are scoped to include or exclude external, insider, and trusted insider APT actors. While TARA does not develop an explicit adversary model, the default TTP scoring model does make assumptions about an adversary's level of sophistication and objectives in the factor weightings that is uses.

MORDA provides alternative techniques to assess CM value: aggregated value, optimization, and cost-benefit. The later approach appears to be similar to the utility/cost (U/C) ratio approach used in TARA to assess CM merit. Like TARA, MORDA provides a framework in which alternative scoring approaches can be used.

Given the limited information available in the public domain about MORDA, it would be premature to conclude that one methodology is substantively better or worse than the other. However it does appear that a TARA assessment would have a more limited scope and require less time and resources to perform than a MORDA assessment of the same system.

4.6.2 Decision Analysis to Counter Cyber Attacks (DACCA)

DACCA was a FY09-FY10 MITRE MOIE to develop a decision analysis process and model to aid in the selection of mitigations for cyber attacks. Like MORDA, DACCA applies a MODA-based analytic approach based on SME assessments of adversary capabilities and objectives, as well as the potential severity of a compromise.

The DACCA methodology constructs models to represent key stakeholders, the adversary, as well as attack classes and impacts. The stakeholder model defines user preferences with respect to continuity of service operation and cyber responses to a cyber attack. The adversary model assumes a sophisticated and resourceful adversary, i.e., the APT. The modeling of attack classes potentially leveraged a variety of sources, including attack trees, catalogs, as well as Red-Team exercises.

The final step in the DACCA information gathering phase is to identify potential response actions for each critical service and attack impact pair. These actions can include combinations of technical solutions, personnel actions, and procedures. In the terminology used in this paper, this step identifies countermeasures (CMs) and their TTP mappings.

DACCA's analytic approach develops estimates of an attack's attractiveness, to the adversary, and its likelihood for success. The attack attractiveness estimate is derived from assumptions made about the adversaries' objectives, resources, and fear of getting caught. The likelihood of success estimate is derived from assumptions made about the ability of the adversary to exploit a vulnerability of the target system.

Two DACCA-developed matrices are used to assess the overall risk associated with each TTP based on the estimates above and the assessed impact level. The Attack Threat Matrix is indexed using the attack attractiveness and likelihood of success estimates to assign an Attack Threat

Level (ATL) rating to the TTP. The ATL value and an assessed impact level estimate are then used to index a Risk Matrix to determine the attack risk level of the TTP. Both matrices are similar to the standard risk cube in their use of ordinal values.

DACCA leverages a separate, MITRE-developed approach to evaluate CMs called PALMA, which stands for Portfolio Analysis Machine. PALMA selects the best combination of countermeasures, referred to as investments, based on criteria that include cost, performance, and/or resource constraints. PALMA can be used to model dependencies and potential conflicts among investment alternatives as well, and provides GUI-based tools that used to test solution alternatives and perform "what if" analysis.

The TARA default TTP scoring model applies a MODA-based analytic approach that utilizes weighted sums to calculate TTP risk scores. The DACCA approach combines factors using a sequence of matrices applied in succession. The TARA scoring model makes use of a range of evaluation criteria, which can be tailored for use in a given assessment. DACCA matrices effectively hardcode evaluation criteria used to assess TTP risk, which limits the ability of DACCA to support new criteria or assign weightings to different criteria.

DACCA estimates TTP risk on an ordinal scale: very high, high, medium, low, and very low. The TARA scoring model calculates a risk score for TTPs in the range [1…5], and then bins them into severity categories: red, yellow or blue based on their risk score.

TARA assessments utilize a catalog of stored TTPs, CMs and TTP/CM mappings, which is maintained through a separate workflow within the TARA methodology. DACCA utilizes TTPs and CMs found in catalogs or identified through red-teaming activities. DACCA's information gathering phase is conducted independently for each assessment, and does not maintain or cultivate the information sources that it utilizes.

The DACCA MOIE demonstrates how an investment portfolio analysis tool (PALMA) [22] can be adapted to the assessment of countermeasures. PALMA's support for modeling of dependencies and conflicts among investments (countermeasures) is one capability that is missing in CRRA.

Both DACCA and TARA have their strengths and weaknesses. These two approaches could be combined in ways that complement each other. One hybrid approach might be to replace the default TTP scoring model with the DACCA analytic approach in a TARA assessment. A second approach might be to replace the default CM scoring model, i.e., U/C ratios, with PALMA tools to assess and select CMs in a TARA assessment.

Use of PALMA to select CMs in TARA was evaluated as part of the FY11 MAE Capstone. The MAE toolset was modified to generate a spreadsheet containing CM selection data for input to the PALMA tool. This spreadsheet includes CM effectiveness and cost data from the MAE catalog. PALMA was able to use this data to produce a graph depicting a range of optimal solutions. However the results would benefit from better calibration between the MAE catalog data and the numerical analysis approach utilized by PALMA.

4.6.3 Common Vulnerability Scoring System (CVSS)

The Common Vulnerability Scoring System (CVSS) provides an open framework for communicating the characteristics and impacts of vulnerabilities. Its quantitative model ensures repeatable accurate measurement while enabling users to see the underlying vulnerability characteristics that were used to generate the scores.

This quantitative model is implemented through the CVSS Calculator, available on the CVSS website, which calculates an overall CVSS score for each CVE using a weighted scoring model that factors in several criteria combined using three (3) separate equations: the base score equation, the temporal equation, and the environmental equation.

The base score equation assesses both the impact and the exploitability of a vulnerability, which is characterized in terms of the attack complexity and the level of adversary proximity and authentication required. The temporal equation considers aspects of the vulnerability that may change over time, i.e., confidence that the vulnerability is exploitable and is being exploited, and whether substantive remediation is generally available. The environmental equation assesses potential loss to an organization and how widespread are its affects.

Direct comparisons can be made between the CVSS calculator and the default TTP scoring model supported in TARA. The CVSS calculator computes CVSS scores based on weighted criteria, which is similar to the approached used in the default TARA scoring model. Some of the same criteria used in the CVSS calculations are also used in the default TTP scoring model, including the base score impact metrics and exploit range. Temporal metrics are optional inputs to the CVSS calculation. Unlike the default TTP scoring model, however, CVSS factors, weightings, and the calculations used cannot be tailored for a given assessment.

Finally, CVSS scores are binned into different severity categories in weekly vulnerability reports published by US-CERT [23]. This binning is similar to the binning applied to TTPs listed in a TARA Threat Matrix.

4.6.4 Microsoft Threat Modeling

In 2003 Microsoft developed a 6-step threat modeling methodology that can be applied early and repeatedly during the system development lifecycle to systematically identify and rate cyber threats. Later stages of this methodology focus on the identification and rating of system threats.

The identification of system-related threats is based on knowledge of the system's design and underlying network architecture. A standard template is used to collect and document information about system threats. These documented threats are rated and prioritized based on the assessed risk that they pose to the system.

The range of threats evaluated in the Microsoft methodology include network threats, e.g., session hijacking, etc., host-based threats, e.g., unauthorized access, etc., and application threats, e.g., buffer overflows, etc.. This methodology applies a threat categorization scheme based on attack objectives called STRIDE, which stands for Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege, to bin these threats.

Groups of countermeasures are associated with each STRIDE threat category. Countermeasure implementation may involve design modifications to systems in development and/or configuration changes in deployed systems. The Spoofing threat category, for example, includes countermeasures such as strong authentication and use of encryption to protect stored secrets and data in transit. The countermeasure for the Elevation of privilege threat category is to apply the principle of least privilege.

The standard template used to document threats specifies the threat target, the attack technique, and a set of countermeasures. The template also includes a risk rating for each threat that is calculated using a set of risk factors referred to as DREAD, which stands for Damage potential, Reproducibility, Exploitability, Affected users, Discoverability.

For the risk calculation, values are assigned to each DREAD factor over the ordinal range: Low, Medium, High, and mapped onto a numeric range in order to calculate the risk score. This numeric risk score is later converted back to an ordinal value: High, Medium, or Low when stored in the template. Aspects of the risk calculation can be tailored for the assessment, including the DREAD factor weightings and the numeric-to-ordinal value mappings.

Like TARA, the objective of the Microsoft methodology is to identify, assess, and mitigate cyber threats early in the system development lifecycle based on knowledge of the system's design and underlying network architecture. Both methodologies deliver recommendations on how to mitigate high risk threats through design modifications and/or configuration changes, depending on the phase of the system lifecycle.

The Microsoft methodology bins threats using a categorization scheme (STRIDE) that focuses specifically on the cyber threat. This scheme may not be well suited to assess non-cyber threats, such as supply chain. TARA uses a broader range of categories that include cyber, EW, and supply chain, which is used to establish the scope of an assessment.

TARA makes use of cataloged TTP, CM, and mapping data. Available literature on the Microsoft methodology does not discuss cataloged TTP data. However its use of CM groupings indicates that persistent knowledge of generic threats and countermeasures is used from one assessment to the next.

DREAD factors correspond to criteria used by TARA to assess TTP risk. Damage potential, the first DREAD factor, is analogous to impact-related TARA TTP risk scoring criteria. In the default TARA scoring model, numeric scores are assigned to criteria and used to calculate a TTP risk score, which is reported as a numeric value in the Threat Matrix. In the Microsoft approach, DREAD factor values are assigned as ordinal values and converted to numeric form in order to perform the risk calculation, which is converted back to an ordinal value for storage in the template.

The association of groups of CMs to STRIVE threat categories is analogous to the TARA TTP/CM mapping table. However the Microsoft approach does not perform a utility/cost based assessment of alternative CMs within a group, as occurs in CRRA. Consequently, recommendations provided from a Microsoft assessment may provide a range of CM alternatives, but no analysis of which CM alternative(s) would be best to implement.

4.7 Areas for Additional Research

One area for additional research is support for more sophisticated CM selection strategies. The default CM selection strategy assumes each CM is independent. This simplification does not reflect the reality that one CM may reduce or cancel the effectiveness of another, may compete for resources, and/or may be dependent on other CMs. In addition, the CM selection strategy arbitrarily sets the minimum level of assurance by defining how many highly effective CMs must be implemented for each TTP. Less effective CMs may be combined in order to reach this minimum level. To support very high assurance requirements, the CM selection strategy could be set to a higher minimum. A parametric approach to representing CM selection strategies could be implemented within the PALMA tool to provide a means for conducting sensitivity analysis for CM selection in a TARA assessment.

A second area for additional research is catalog development that supports new applications of the TARA assessment approach. The current MAE catalog focuses on cyber-related TTPs and design-time CMs to support assessments within in the system acquisition lifecycle. TARA support for PPP development would recommend program-level CMs to mitigate TTPs associated

with ex-filtration of CPI, reverse engineering of critical technologies, and/or supply chain attacks. TARA support for operational cyber defense would focus on a range of TTPs and CMs specific to the operational context.

Appendix A Acronym List

AC	Asset Class
ACL	Access Control List
APT	Advanced Persistent Threat
ATL	Attack Threat Level
BGAN	Broadband Global Area Network
BIOS	Basic Input/Output System
C&A	Certification and Accreditation
CAPEC	Common Attack Pattern Enumeration and Classification
CDR	Critical Design Review
CJA	Crown Jewels Analysis
CM	Countermeasure
CMID	Countermeasure ID
CNSS	Committee on National Security Systems
COTS	Commercial off-the-Shelf
CPI	Critical Program Information
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
CWE	Common Weakness Enumeration
CRRA	Cyber Risk Remediation Analysis
CTSA	Cyber Threat Susceptibility Analysis
DACCA	Decision Analysis to Counter Cyber Attacks
DHS	Department of Homeland Security
DIACAP	Defense Information Assurance Certification and Accreditation Process
DISA	Defense Information Systems Agency
DMZ	Demilitarized Zone
DoD	Department of Defense
DODI	Department of Defense Instruction
DNS	Domain Name Service
DREAD	Damage, Reproducibility, Exploitability, Affected users, Discoverability
DTD	Document Type Definition/Declaration
ESE	Enterprise Systems Engineering
EW	Electronic Warfare
FFRDC	Federally Funded Research and Development Center
FHSS	Frequency Hopping Spread Spectrum
FY	Fiscal Year
GUI	Graphical User Interface
HTTP	Hypertext Transfer Protocol
IA	Information Assurance

IC	Intelligence Community
IGMP	Internet Group Management Protocol
IIS	Internet Information Services
INCOSE	International Council on Systems Engineering
IP	Internet Protocol
ISSE	Information System Security Engineering
IT	Information Technology
JSON	JavaScript Object Notation
LAN	Local Area Network
LOE	Level of Effort
MA	Mission Assurance
MAE	Mission Assurance Engineering
MI	Mission Impact
MODA	Multi-Oriented Decision Analysis
MOIE	Mission-Oriented Investigation and Experimentation
MORDA	Mission Oriented Risk and Design Analysis
NET	Network Equipment Technology
NIST	National Institute of Standards and Technology
NMS	Network Management System
OS	Operating System
OSPF	Open Shortest Path First
PALMA	Portfolio Analysis Machine
PDR	Preliminary Design Review
PIM	Protocol Independent Multicast
PKI	Public Key Infrastructure
PoE	Power over Ethernet
PPP	Program Protection Planning
QoS	Quality of Service
RAMBO	Resilient Architecture for Mission Assurance and Business Objectives
SAB	Air Force Scientific Advisory Board
SAM	Service Aware Manager
SAMAE	System/Acquisition Mission Assurance Engineering
SEG	(MITRE) Systems Engineering Guide
SME	Subject Matter Expert
SNMP	Simple Network Management Protocol
SOAP	Simple Object Access Protocol
SOCRATES	Security Optimization Countermeasure Risk and Threat Evaluation System
SOP	Standard Operating Procedure
SP	Special Publication
STA	System Threat Assessment
SQL	Structured Query Language

STIG	(DISA) Security Technical Implementation Guide
STRIDE	Spoofing identity, Tampering with data, Repudiation, Information disclosure, Denial of service, Elevation of privilege
TARA	Threat Assessment & Remediation Analysis
TTP	Tactics, Techniques, and Procedures
U/C	Utility to Cost (Ratio)
UDDI	Universal Description Discovery and integration
URL	Uniform Resource Locator
USAF	United States Air Force
VoIP	Voice over Internet Protocol
VRF	Virtual Routing and Forwarding
VX	Voice Exchange
XML	Extensible Markup Language
XSLT	Extensible Style sheet Language Transformations

Appendix B MAE Terminology

Term	Definition
Advanced Persistent Threat (APT)	An adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors (e.g., cyber, physical, and deception). These objectives typically include establishing and extending footholds within the information technology infrastructure of the targeted organizations for purposes of ex-filtrating information, undermining or impeding critical aspects of a mission, program, or organization; or positioning itself to carry out these objectives in the future. The advanced persistent threat: (i) pursues its objectives repeatedly over an extended period of time; (ii) adapts to defenders' efforts to resist it; and (iii) is determined to maintain the level of interaction needed to execute its objectives [3].
Adversary	A party acknowledged as potentially hostile to a friendly party and against which the use of force may be envisaged. (Inside Threat) An entity with authorized access that has the potential to harm an information system through destruction, disclosure, modification of data, and/or denial of service. (Outside threat) An unauthorized entity from outside the domain perimeter that has the potential to harm an Information System through destruction, disclosure, modification of data, and/or denial of service [17].
Counter Measure (CM)	Actions, devices, procedures, or techniques that meet or oppose(i.e., counters) a threat, a vulnerability, or an attack by eliminating or preventing it, by minimizing the harm it can cause, or by discovering and reporting it so that corrective action can be taken [17].
Criticality	A metric used to describe the consequence of loss of an asset, based on the effect the incapacitation or destruction of the asset would have on DoD operations and the ability of the Department of Defense to fulfill its missions [24].
Cyber Attack	An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information [17].
Dependency	A relationship or connection in which one entity is influenced or controlled by another entity [25].
Enterprise Systems Engineering	The body of knowledge, principles, and disciplines related to the analysis, design, implementation and operation of all elements associated with an enterprise [26].
Fight Through	The process through which a war fighter achieves the desired mission effects in the presence of deficiencies in operational capability caused by an adversary's activities in cyberspace [2].
Impact	The magnitude of harm that can be expected to result from the consequences of unauthorized disclosure of information, unauthorized modification of information, unauthorized destruction of information, or loss of information or information system availability [27].

Mission Assurance	Measures to accomplish objectives of missions in the presence of information assurance compromises [2].
Threat	Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service [17].
Adversarial TTP	A sequence of steps performed by an adversary in the course of conducting a cyber attack.
Vulnerability	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source [17].
Weakness	The state of being unable to resist external force or withstand attack. (Source: Merriam-Webster dictionary)

Appendix C MAE Catalog Details

The MAE catalog data model is illustrated by the following diagram.

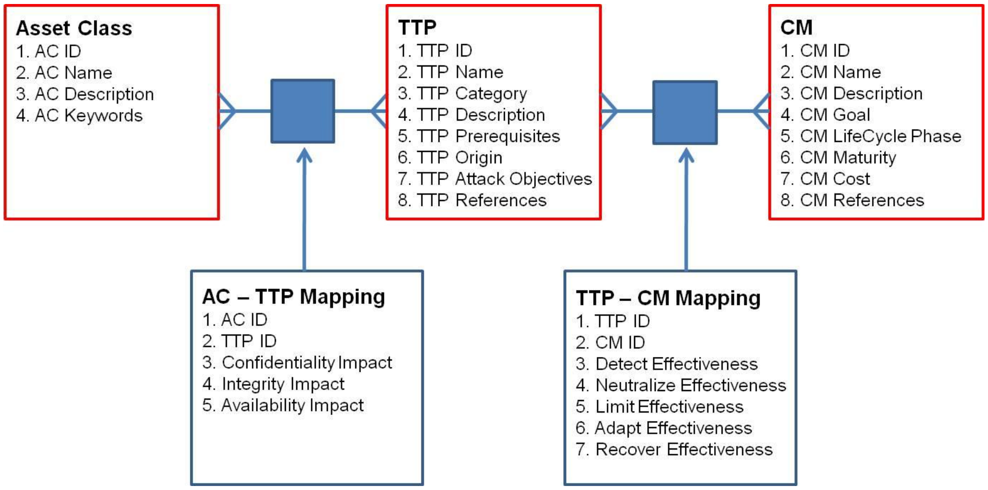

Figure 18 MAE Data Model

C.1 Data Dictionary

TTP Category	
Cyber	An attack targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling its computing environment or infrastructure;
Physical	A Physical attack is the use of physical force to impair or destroy an asset or exercise control over one or more individuals.
Social Engineering	Social Engineering – The act of manipulating people into performing actions or divulging confidential information.
Supply Chain	An attacker tampers with a physical asset during manufacture or while it is in transit to the end user. A supply chain attack requires physical access.
Electronic Warfare	Electronic Warfare – An attacker uses the electromagnetic spectrum or directed energy to control the spectrum, attack a target, or impede an attack.
TTP Origin	
External	An attacker from outside the organization being attacked.
Insider	An attacker inside the organization being attacked.
Trusted Insider	An attacker with administrative privileges inside the organization being attacked.
TTP Objective	
Recon	TTP provides adversary ability to scout and survey an organization's cyber assets to enable it to identify potentially exploit weaknesses and/or gain insight into security methods.
Penetration	TTP provides adversary ability to breach the security controls of a cyber asset.

Implantation	TTP installs/establishes itself in the asset in preparation for carrying out attacks or implanting itself further into the other assets.
Exfiltration	TTP takes actions resulting in the release and/or transfer of information to an unauthorized entity.
Disruption	TTP takes actions that result in the interruption, degradation, and/or corruption of the cyber asset’s services or information.
Destruction	TTP takes actions that result in the elimination/obliteration of a cyber asset.
CM Goal	
Detect	Identify/uncover the actions or presence of a TTP.
Limit	Materially reduce or constrain the effectiveness of a successfully executed TTP.
Adapt	Adjust, change or reconfigure cyber assets in face of adversary attacks to mitigate the possibility of success of adversary TTPs.
Neutralize	Stop the successful execution of a TTP.
Recover	Facilitate the reconstitution of cyber assets from the successful execution of the TTP.
CM Scope	
Very limited	This CM is applicable to a very limited number of TTPs.
Limited	This CM is applicable to a limited number of TTPs.
Significant	This CM is applicable to a significant number of TTPs.
Large	This CM is applicable to a large number of TTPs.
Very large	This CM is applicable to a very large number of TTPs.
CM Form	
Methodology	Countermeasure implemented in the form of a new or revised SDLC process, practice, activity or procedure.
Requirements	Countermeasure implemented in the form of new or modified system requirements.
Design	Countermeasure implemented in the form of new or modified system design.
Implementation	Countermeasure implemented in the form of discrete software or hardware changes to a cyber asset.
Fielding	Countermeasure implemented in the form of revised installation or testing procedures.
Operation	Countermeasure implemented in the form of configuration changes or revised operating procedures.
Disposal	Countermeasure implemented in the form of operating procedures relating to the disposal of a system.
CM Maturity	
Unproven	Cyber security solutions that are in the concept, research, prototype, or proof-of-concept stage. Development has not yet started on these unproven cyber security solutions.
Developing	Cyber security solutions that are in development but have not been widely tested and are not employed in operational environments.
Emerging	Cyber security solutions that are available but not in widespread usage today. Emerging cyber security solutions involve early adoption of emerging cyber security technology or application of existing technology

	in a new manner.
Widespread	Commercial, leading edge cyber security solutions that are available and in widespread use.

C.2 Representative TTPs

The following is a partial listing of cyber TTPs from the MAE Catalog.

TTP ID	TTP Name
T000001	Malicious BIOS code allows unsigned updates
T000006	Compromised update server distributes malicious BIOS
T000009	Session Credential Falsification through Prediction
T000010	HTTP Request Smuggling
T000011	Lifting Data Embedded in Client Distributions
T000012	Postfix, Null Terminate, and Backslash
T000013	Exploiting Trust in Client
T000014	Accessing, Intercepting, and Modifying HTTP Cookies
T000015	Cross Site Request Forgery (Session Riding)
T000016	Simple Script Injection
T000017	Subvert Code-signing Facilities
T000020	XQuery Injection
T000021	Man in the Middle Attack
T000022	Cryptanalysis
T000023	Cross Site Tracing
T000024	Malicious Software Update
T000026	Accessing Functionality Not Properly Constrained by ACLs
T000027	Manipulating Input to File System Calls
T000028	Manipulating User-Controlled Variables
T000029	Session Side jacking
T000030	JSON Hijacking (aka JavaScript Hijacking)
T000032	XPath Injection
T000034	OS Command Injection
T000035	Reflection Attack in Authentication Protocol
T000036	Log Injection-Tampering-Forging
T000037	Accessing Modifying or Executing Executable Files
T000038	Leverage Executable Code in Non-executable Files
T000039	Exploitation of Session Variables, Resource IDs and other Trusted Credentials
T000040	File System Function Injection, Content Based

T000041	Leveraging Race Conditions
T000043	Fraudulent PKI certificates
T000044	Phishing
T000049	Buffer Overflow
T000050	Forced Integer Overflow, renamed Forced Native Type Overflow
T000051	Manipulating Writeable Configuration Files
T000054	SQL Injection through SOAP Parameter Tampering
T000055	Target Programs with Elevated Privileges
T000056	Subverting Environment Variable Values
T000057	Leveraging/Manipulating Configuration File Search Paths
T000058	Manipulating Writeable Terminal Devices
T000059	Using Meta-characters in E-mail Headers to Inject Malicious Payloads
T000060	Passing Local Filenames to Functions That Expect a URL
T000061	Embedding NULL Bytes
T000063	Reusing Session IDs (aka Session Replay)
T000064	SQL Injection
T000065	Blind SQL Injection
T000066	Web Server/Application Fingerprinting
T000067	XML Ping of Death
T000070	Resource Depletion through DTD Injection in a SOAP Message
T000071	SOAP Array Overflow
T000072	Using Unpublished Web Service APIs
T000073	HTTP Response Splitting
T000075	Detect Unpublicized Web Services
T000076	HTTP Verb Tampering
T000077	SOAP Parameter Tampering
T000078	Flash Parameter Injection
T000079	Spoofing of UDDI Messages
T000080	Parameter Injection
T000081	HTTP Response Smuggling

C.3 Representative CMs

The following is a partial listing of CMs from the MAE Catalog.

CM ID	CM Name
C000002	Verify BIOS image write protection
C000003	Verify recovery process to restore last-known-good BIOS image
C000007	Verify BIOS update does not result in buffer overflows
C000010	Restrict admin access to device
C000012	Enforce the 2-man rule when performing critical administrative functions
C000013	Conduct independent verification of software image once installed
C000015	Verify BIOS implemented security controls after BIOS image update
C000018	Use checksums to verify the integrity of downloaded BIOS image updates
C000020	Restrict access to the BIOS update server
C000021	Use newer version of SNMP protocol
C000022	Isolate network management traffic to internal network
C000025	Configure web servers to utilize strict parsing
C000027	Terminate client sessions after each request
C000028	Mark all sensitive web pages as non-cacheable
C000030	Conduct threat modeling
C000034	Reduce attack surface
C000041	Use same character encoding
C000045	Utilize high quality session IDs
C000047	Encrypt session cookies
C000049	Enforce client authentication
C000051	Use digital signatures
C000058	Use a cryptographic token to bind an action to a request
C000059	Enable use of the HTTP Referrer header field
C000061	Require user confirmation when action involves sensitive data
C000062	Disable client side scripting
C000064	Do not deploy content proxies that mask where data originates from
C000065	Sanitize outbound content
C000067	Avoid Relying on User Controllable Flags and Variables
C000068	Verify use of Unicode data

C000074	Perform Security Checks After Decoding
C000075	Do not make decisions based on filename
C000077	Perform xml parsing with minimal privileges
C000079	Only accept PKI credentials from a trusted certificate authority
C000081	Use Strong mutual authentication
C000083	Use cryptography properly
C000084	Disable HTTP TRACE support
C000086	Treat each exposed API as an attack vector
C000087	Accept hyperlinks/attachments from trusted sources only
C000089	Perform range checks on numeric input
C000090	Validate input fields use of NULL, escape, backslash, meta, and control characters
C000091	Apply blacklist and whitelist validation in combination
C000092	Apply parser-based validation for structured data
C000093	Merge data streams prior to validation
C000094	Validate data exchanges across language boundaries
C000095	Convert input to canonical form before validating
C000096	Use vetted runtime libraries
C000097	Validate library source code to establish trust
C000098	Apply strong output encoding
C000099	Utilize common encoding formats
C000100	Use character encoding formats consistently
C000101	Verify buffer sizes
C000102	Verify message size data
C000103	Match buffer size to data input size
C000104	Conduct system-wide data flow analysis
C000105	Apply static code analysis to identify defects
C000106	Apply dynamic runtime analysis tools to identify defects
C000109	Apply error checking when accessing a protected resource
C000110	Keep it simple
C000111	Prohibit use of dangerous functions

Appendix D MAE Toolset Details

Web forms used to manage MAE Catalog data include the TTP management interface, the CM management interface, and the Asset Class management interface. Screen shots of these web forms are illustrated in Figures 19, 20, and 21, respectively.

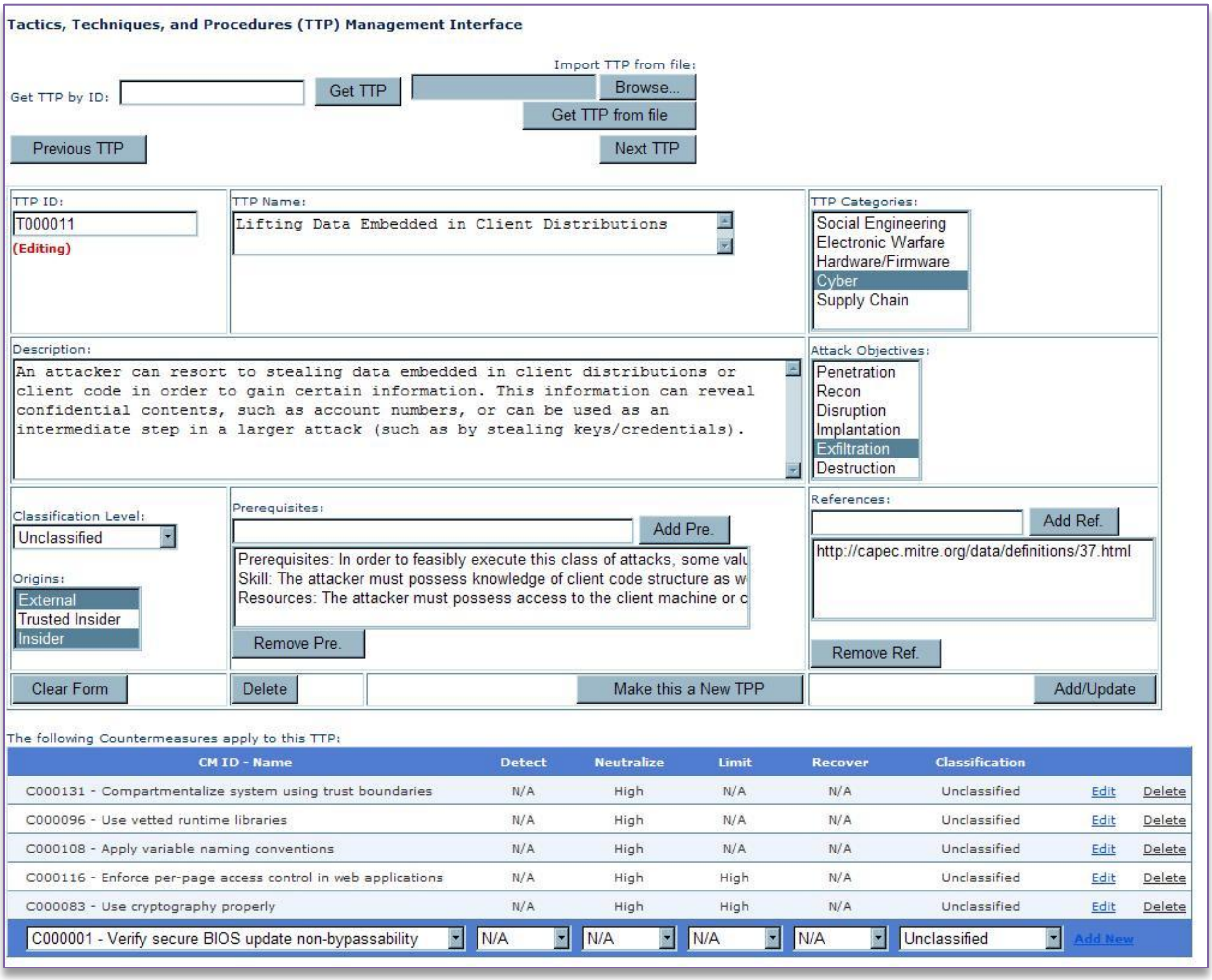

Figure 19 TTP Management Interface

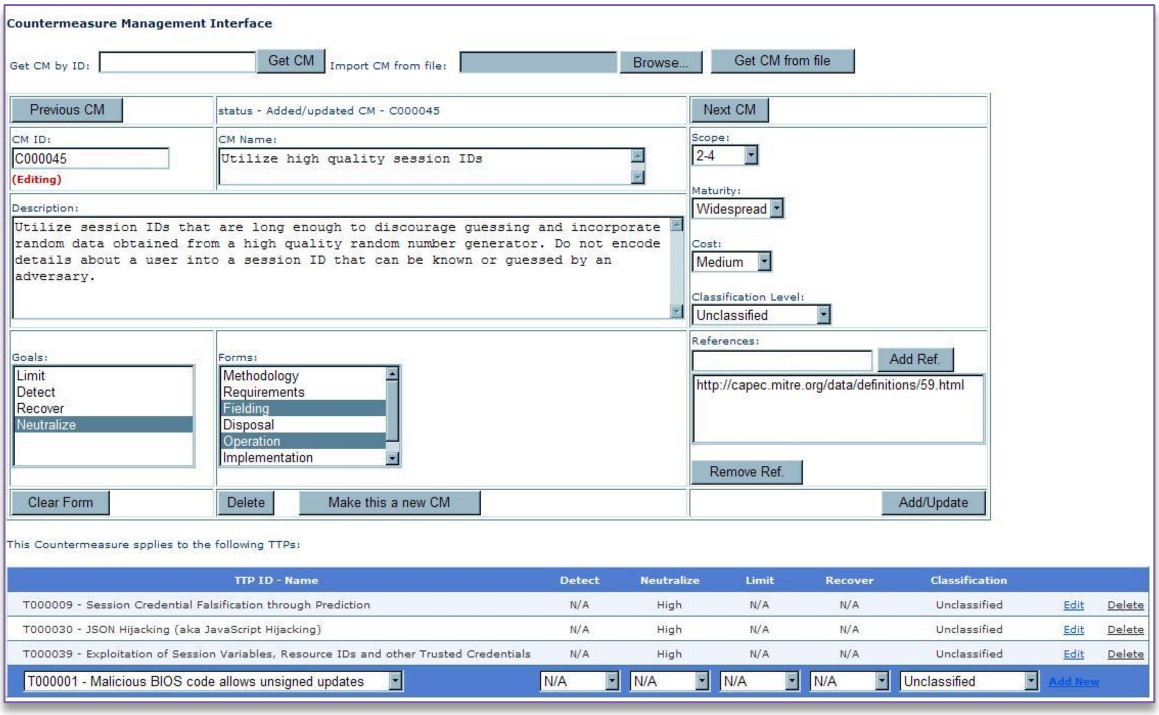

Figure 20 CM Management Interface

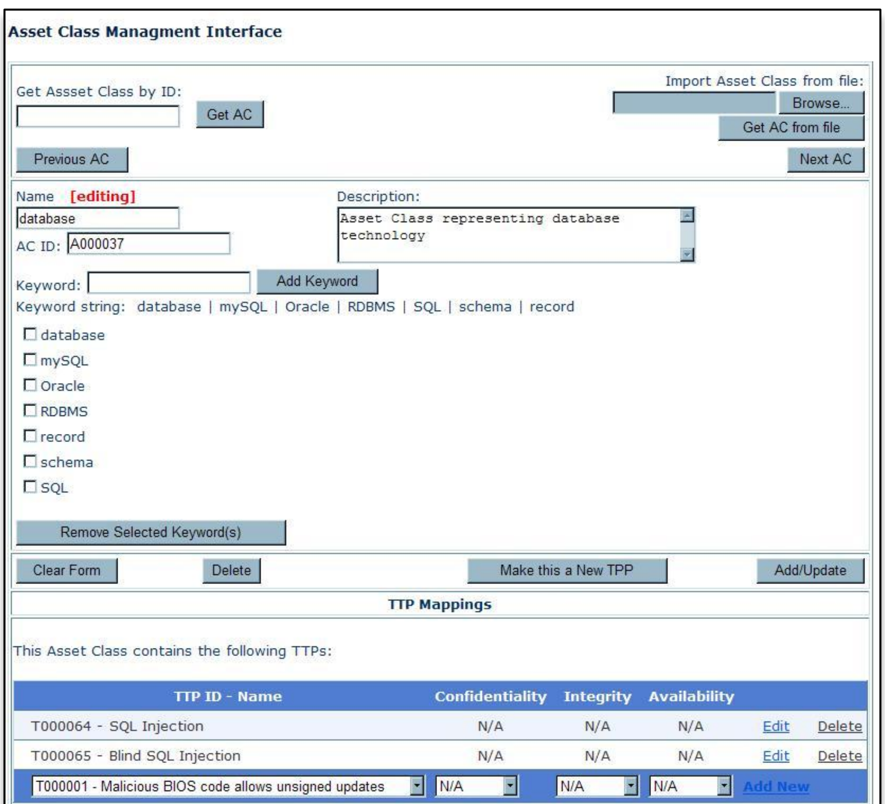

Figure 21 Asset Class Management Interface

Appendix E References and Links

1. Wynn, J., Montella, L., “Cyber Threat Susceptibility Analysis (TSA) Methodology”, Version 2.0, MITRE Technical Report (MTR) 100379, October 2010.
2. "Defending and Operating in a Contested Cyber Domain", USAF Scientific Advisory Board, SAB-TR-08-01, August 2008.
3. NIST Special Publication 800-39, “Integrated Enterprise-Wide Risk Management” Draft, December 2010.
4. Hastings, G., Montella, L., and Watters, J., “MITRE Crown Jewels Analysis Process”, MITRE Technical Report MTR090088, 8 April 2009.
5. Bodeau, D., Graubart, R., and Fabius-Greene, J., Improving Cyber Security and Mission Assurance via Cyber Preparedness (Cyber Prep) Levels, The MITRE Corporation, 2009, PR 09-4656, http://www.mitre.org/work/tech_papers/2010/09_4656/09_4656.pdf
6. Goldman, H., Building Secure, Resilient Architectures for Cyber Mission Assurance. Paper presented at the 2010 Secure & Resilient Cyber Architectures Conference, McLean, VA.
7. Buckshaw, D., Parnell, G., et. al., “Mission Oriented Risk and Design Analysis of Critical Information Systems (MORDA)”, Military Operations Research, V10, 2005, pp. 19-38,
8. Decision Analysis to Counter Cyber Attacks (DACCA), http://www.mitre.org/news/events/exchange09/03X97563.pdf
9. Common Vulnerability Scoring System (CVSS), http://nvd.nist.gov/cvss.cfm
10. Meier, J.D., Mackman, A., et. al, Improving Web Application Security: Threats and Countermeasures, Microsoft Patterns and Practices, Chapter 2, http://msdn.microsoft.com/en-us/library/aa302418.aspx, January 2006.
11. Meier, J.D., Mackman, A., et. al., Threat Modeling, Microsoft Patterns and Practices, Chapter 3, http://msdn.microsoft.com/en-us/library/ff648644.aspx, June 2003.
12. Common Attack Pattern Enumeration and Classification (CAPEC), http://capec.mitre.org/.
13. Common Weakness Enumerations (CWE), http://cwe.mitre.org/.
14. Common Vulnerability Enumeration (CVE), http://cve.mitre.org/.
15. DoD Instruction 8500.2, "Information Assurance (IA) Implementation", ASD(C3I), February 2003.
16. DISA Security Technical Implementation Guides (STIGs), http://iase.disa.mil/stigs/index.html
17. CNSS Instruction 4009, “National Information Assurance (IA) Glossary”, April 2010.
18. Blackhat, http://www.blackhat.com/
19. SchmooCon, http://www.shmoocon.org/
20. Apache Solr Project, http://lucene.apache.org/solr/
21. Parnell, G. S., Multi-objective Decision Analysis, Wiley Handbook of Science & Technology for Homeland Security, John G. Voeller, Editor, 2008.
22. Moynihan, R., "Investment Analysis using the Portfolio Analysis Machine (PALMA) Tool", MITRE Corporation, July 2005.
23. US-CERT Cyber Security Bulletins, http://www.us-cert.gov/cas/bulletins/

24. DoD Instruction 3020.45, "Defense Critical Infrastructure Program (DCID) Management", USD(P), April 2008.
25. DoD Directive 3020.40, "DoD Policy and Responsibilities for Critical Infrastructure", USD(P), January 2010.
26. International Council on Systems Engineering (INCOSE), "Systems Engineering Handbook", v3.1, INCOSE-TP-2003-002-03.1, August 2007.
27. NIST Special Publication 800-30, "Risk Management Guide for Information Technology Systems", July 2002.